Isotypic Decomposition of the Cohomology and Factorization of the Zeta Functions of Dwork Hypersurfaces

Philippe Goutet

Isotypic Decomposition of the Cohomology and Factorization of the Zeta Functions of Dwork Hypersurfaces

Philippe Goutet

December 10, 2009

Abstract

The aim of this article is to illustrate, on the Dwork hypersurfaces $x_1^n+\cdots+x_n^n-n\psi x_1\dots x_n=0$ (with n an integer ≥ 3 and $\psi\in\mathbb{F}_q^*$ a parameter satisfying $\psi^n\neq 1$), how the study of the representation of a finite group of automorphisms of a hypersurface in its etale cohomology allows to factor its zeta function.

1 Introduction

Let n be an integer ≥ 3 and $\mathbb{F}_q$ a finite field of characteristic $p\neq 2$ not dividing n; to simplify the results, we will assume that $q\equiv 1 \mod n$. We consider the projective hypersurface $X_\psi\subset\mathbb{P}^{n-1}_{\mathbb{F}_q}$ given by

$$x_1^n+\cdots+x_n^n-n\psi x_1\dots x_n=0,$$

where ψ is a non zero parameter belonging to $\mathbb{F}_q$. The zeta function of X_ψ is defined as

$$Z_{X_\psi/\mathbb{F}_q}(t)=\exp\biggl(\sum_{r=1}^{+\infty}\#X_\psi(\mathbb{F}_{q^r})\frac{t^r}{r}\biggr).$$

We assume that $\psi^n\neq 1$, so that $\overline{X}_\psi=X_\psi\otimes_{\mathbb{F}_q}\overline{\mathbb{F}}_q$ is nonsingular. As X_ψ is a non-singular hypersurface of $\mathbb{P}^{n-1}$, we know that the dimension of the etale ℓ-adic cohomology spaces $H^i_{\mathrm{et}}(\overline{X}_\psi,\mathbb{Q}_\ell)$ is zero for $i>2n-4$ or $i<0$ and that, for $0\leq i\leq 2n-4$,

$$\dim H^i_{\mathrm{et}}(\overline{X}_\psi,\mathbb{Q}_\ell)=\begin{cases}\delta_i & \text{if } i\neq n-2,\\ \delta_i+\frac{(n-1)^n+(-1)^n(n-1)}{n} & \text{if } i=n-2,\end{cases}$$

where $\delta_i=0$ if i is odd and $\delta_i=1$ if i is even (see §2.2). As we will recall in Remark 2.3 page 3, the zeta function of X_ψ is related to how the Frobenius acts on $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi,\mathbb{Q}_\ell)$.

We set

$$A=\{(\zeta_1,\dots,\zeta_n)\in\boldsymbol{\mu}_n(\mathbb{F}_q)^n\mid\zeta_1\dots\zeta_n=1\}/\{(\zeta,\dots,\zeta)\};$$
$$\hat{A}=\{(a_1,\dots,a_n)\in(\mathbb{Z}/n\mathbb{Z})^n\mid a_1+\cdots+a_n=0\}/\{(a,\dots,a)\},$$

and denote by $[\zeta_1,\dots,\zeta_n]$ the class of $(\zeta_1,\dots,\zeta_n)$ in A and $[a_1,\dots,a_n]$ that of $(a_1,\dots,a_n)$ in $\hat{A}$. We will identify the group $\hat{A}$ with the group of characters of A taking values in $\mathbb{F}_q^*$. The group A

2000 Mathematical Subject Classification: Primary 14G10; Secondary 11G25, 14G15, 20C05.
Keywords: Zeta function factorisation, Dwork hypersurfaces, isotypic decomposition.

acts on X_ψ by coordinatewise multiplication; the symmetric group $\mathfrak{S}_n$ acts on the right on X_ψ by permutation of the coordinates

$$[x_1 : \ldots : x_n]^\sigma = [x_{\sigma(1)} : \ldots : x_{\sigma(n)}],$$

and on the left on A and $\hat{A}$ by

$$\begin{aligned} {}^\sigma[\zeta_1, \ldots, \zeta_n] &= [\zeta_{\sigma^{-1}(1)}, \ldots, \zeta_{\sigma^{-1}(n)}]; \\ {}^\sigma[a_1, \ldots, a_n] &= [a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)}]. \end{aligned}$$

The semidirect product $G = A \rtimes \mathfrak{S}_n$ acts on the right on X_ψ, and hence on the left on $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)$ as the functor $g \mapsto g^*$ is contravariant.

The aim of this article is to describe the structure of $H^{n-2}_{\mathrm{et}}(X_\psi, \mathbb{Q}_\ell)$ as a $\mathbb{Q}_\ell[G]$-module in order to deduce a factorization of the zeta function of X_ψ. More precisely, we will show that the primitive part of $H^{n-2}_{\mathrm{et}}(X_\psi, \mathbb{Q}_\ell)$ (as defined in §2.2) admits an isotypic decomposition

$$\bigoplus_{a,\omega} W_{a,\omega} \otimes_{D_a} V_{a,\omega},$$

where a describes $(\mathfrak{S}_n \times (\mathbb{Z}/n\mathbb{Z})^\times)\backslash\hat{A}$, ω belongs to a certain set of roots of unity (see Corollary 5.12 page 19), $W_{a,\omega}$ is a simple $\mathbb{Q}[G]$-module which is independent of ℓ, D_a is the division ring $\mathrm{End}_{\mathbb{Q}[G]}(W_{a,\omega})^{\mathrm{opp}}$, and $V_{a,\omega}$ is a free module over $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ whose rank is independent of ℓ. Because the Frobenius stabilizes these isotypic spaces, its characteristic polynomial splits in as many factors (the idea to use this method is inspired by an argument given in [Hulek et al., 2006, §6.2]).

The first step is to decompose the $\overline{\mathbb{Q}}_\ell[G]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)$; we follow the same method Brünjes used for the case $\psi = 0$ (Fermat hypersurface), but, thanks to a more powerful trace formula, we avoid the tedious induction of [Brünjes, 2004, Proposition 11.5]. Our methods can be generalized to other families of hypersurfaces, allow us to obtain factorizations slightly finer than those of Kloosterman [2007] (who uses the p-adic Monsky-Washnitzer cohomology), and also allow us to express each factor as the norm of a polynomial with coefficients in a certain finite extension of $\mathbb{Q}$, hence explaining a numerical observation of Candelas, de la Ossa and Rodriguez-Villegas in the case $n = 5$ where this extension is $\mathbb{Q}(\sqrt{5})$ (see [Candelas et al., 2003, Table 12.1 page 133][1]). Let us also mention that, in a recent article, Katz [2009] studies the action of A (but not of $A \rtimes \mathfrak{S}_n$) on the cohomology of X_ψ and establishes a motivic link between X_ψ and objects of hypergeometric type.

The article is organized as follows. After preliminaries (§2), we describe the structure of $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)$ as a $\overline{\mathbb{Q}}_\ell[A]$-module (§3) and then as a $\overline{\mathbb{Q}}_\ell[G]$-module (§4). We then deduce the structure of the $\mathbb{Q}_\ell[G]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)$ (§5) and explain the link between this structure and the existence of a factorisation of the zeta function of X_ψ (§6). An index of all notations introduced in the article is given in §A and a table of the main formulas appears in §B.

2 Preliminaries

We begin by recalling a Lefschetz-type trace formula by Deligne and Lusztig which allows to express the alternating sum of the traces of an automorphism on the ℓ-adic cohomology spaces as the Euler–Poincaré characteristic of the fixed-point scheme of this automorphism. We then recall the value of this Euler–Poincaré characteristic in the cases we will encounter in what follows (smooth projective hypersurfaces). Finally, we link the trace of an element of G to the Euler–Poincaré characteristic of a subscheme of fixed points.

[1] They make this observation only in the case $\psi = 0$, but their numerical data in §13.3 suggests the same phenomenon happens when $\psi \neq 0$ and $q \equiv 1 \mod 5$.

2.1 Lefschetz trace formula

Let us recall that the Euler–Poincaré characteristic of a proper scheme over $\overline{\mathbb{F}}_p$ is given by

$$\chi(X) = \sum_{i=0}^{2\dim X} (-1)^i \dim H^i_{\mathrm{et}}(X, \mathbb{Q}_\ell),$$

where ℓ is a prime number $\neq p$. It is an integer independent of ℓ.

Theorem 2.1. *Let X be a proper scheme over $\overline{\mathbb{F}}_p$. If f is an automorphism of X of finite order prime to p, and if X^f denotes the fixed-point subscheme of f of the scheme X, then*

$$\sum_{i=0}^{2\dim X} (-1)^i \operatorname{tr}(f^*|H^i_{\mathrm{et}}(X, \mathbb{Q}_\ell)) = \chi(X^f).$$

Proof. See [Deligne and Lusztig, 1976, Theorem 3.2, page 119]. □

2.2 Euler–Poincaré characteristic of a non-singular hypersurface

In this §2.2, exceptionally, we do not assume that $n \geq 3$.

Theorem 2.2 (Hirzebruch formula)**.** *Let n be an integer ≥ 1 and $f \in \overline{\mathbb{F}}_p[x_1, \dots, x_n]$ a homogeneous polynomial of degree d such that f, $\frac{\partial f}{\partial x_1}$, $\dots$, $\frac{\partial f}{\partial x_n}$ have no common zero in $\overline{\mathbb{F}}_p^n$ except $(0, \dots, 0)$. Then the hypersurface $X \subset \mathbb{P}^{n-1}_{\overline{\mathbb{F}}_p}$ defined by $f = 0$ is non-singular (and irreducible if $n \geq 3$) and its Euler–Poincaré characteristic is*

$$\chi(X) = (n-1) + \frac{(1-d)^n + (d-1)}{d}.$$

Proof. If $n \geq 3$, we use Corollary 7.5.(*iii*) of [SGA5, exposé VII]: indeed, the subscheme X of $\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_p}$ is smooth, connected and of dimension $n-2$; its Euler–Poincaré characteristic is hence

$$\begin{aligned}\chi(X) &= d \sum_{i=0}^{n-2} (-1)^{n-i} \binom{n}{i} d^{n-2-i} = \frac{1}{d} \sum_{i=0}^{n-2} (-1)^{n-i} \binom{n}{i} d^{n-i} \\ &= \frac{(1-d)^n + nd - 1}{d},\end{aligned}$$

which is the announced formula. If $n = 2$, the hypersurface X of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$ consists of d distinct points and so $\chi(X) = d$, which shows the result as $(2-1) + \frac{1}{d}[(1-d)^2 + (d-1)] = d$. Finally, if $n = 1$, $X = \varnothing$ and so $\chi(X) = 0$, which also shows the result in this case. □

Remark 2.3. When $n \geq 3$, Theorem 2.2 can be refined as follows. We keep the same notations and denote by j the canonical injection $X \to \mathbb{P}^{n-1}_{\overline{\mathbb{F}}_p}$. By the Weak Lefschetz Theorem, (see for example [Freitag and Kiehl, 1988, Corollary 9.4, page 106]), for $i < n-2$ (respectively $i = n-2$), the linear map $j^*\colon H^i_{\mathrm{et}}(\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell) \to H^i_{\mathrm{et}}(X, \mathbb{Q}_\ell)$ is bijective (respectively injective). If we set $\delta_i = 0$ if i odd and $\delta_i = 1$ if i is even, we thus have $\dim H^i_{\mathrm{et}}(X, \mathbb{Q}_\ell) = \delta_i$ for $i < n-2$, and this result stays valid for $n-2 < i \leq 2(n-2)$ by Poincaré duality. For $i = n-2$, the image of the map $j^*\colon H^{n-2}_{\mathrm{et}}(\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell) \to H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)$ has dimension δ_i. We will denote it by $H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)^{\mathrm{inprim}}$ and set $H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)^{\mathrm{prim}} = H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)/H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)^{\mathrm{inprim}}$. Because the Frobenius acts as the multiplication by $q^{(n-2)/2}$ on $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{inprim}}$ and by multiplication by q^i on each $H^{2i}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)$, we have

$$Z_{X_\psi/\mathbb{F}_q}(t) = \frac{\det(1 - t\operatorname{Frob}^*|H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}})^{(-1)^{n-1}}}{(1-t)(1-qt)\dots(1-q^{n-2}t)}.$$

2.3 Character of G acting on $H^{n-2}_{\mathbf{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathbf{prim}}$

The isomorphism class of a $\mathbb{Q}_\ell[G]$-module is completely determined by its character. In this §2.3, we will express in terms of Euler–Poincaré characteristics the values of the character of the $\mathbb{Q}_\ell[G]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}}$ for the elements $g \in G$ which are of order prime to p.

Lemma 2.4. *Each $g \in G$ acts as the identity on $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{inprim}}$ and on $H^i_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)$ when $i \neq n-2$.*

Proof. As g is the restriction of an automorphism of $\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_q}$, it results from Remark 2.3 and the following lemma. □

Lemma 2.5. *If h is an automorphism of $\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_q}$, then h^* acts as the identity on $H^i_{\mathrm{et}}(\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ for all i.*

Proof. The group $PGL_n(\overline{\mathbb{F}}_q)$ acts on the right on $H^i_{\mathrm{et}}(\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ by $u \mapsto u^*$; as $H^i_{\mathrm{et}}(\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ is of dimension 0 or 1, this action is by homothety, and thus factors by an abelian quotient of $PGL_n(\overline{\mathbb{F}}_q)$. Since $\overline{\mathbb{F}}_q$ is algebraically closed, $PGL_n(\overline{\mathbb{F}}_q)$ is equal to its commutator subgroup and thus has no nonzero abelian quotient. Hence, for all $u \in PGL_n(\overline{\mathbb{F}}_q)$, $u^* = \mathrm{Id}$. □

Theorem 2.6. *If $g \in G$ is of order prime to p, then*

$$\mathrm{tr}(g^* | H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}}) = (-1)^{n-1}\Big((n-1) - \chi(\overline{X}^g_\psi)\Big). \tag{2.1}$$

Proof. Using the trace formula of Theorem 2.1, we can write

$$\sum_{i=0}^{2\dim X} (-1)^i \,\mathrm{tr}(g^* | H^i_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)) = \chi(\overline{X}^g_\psi).$$

By Lemma 2.4, we have (with, as previously, $\delta_i = 0$ if i is odd and $\delta_i = 1$ if i is even)

$$\mathrm{tr}(g^* | H^i_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)) = \begin{cases} \delta_i & \text{if } i \neq n-2, \\ \delta_i + \mathrm{tr}(g^* | H^i_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}}) & \text{if } i = n-2, \end{cases}$$

and thus

$$\chi(\overline{X}^g_\psi) = (n-1) + (-1)^{n-2}\,\mathrm{tr}(g^* | H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}}),$$

which is exactly the announced formula. □

3 Action of A on $H^{n-2}_{\mathbf{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathbf{prim}}$

The irreducible representations over $\overline{\mathbb{Q}}_\ell$ of the finite abelian group A are its characters (of degree 1). Finding the structure of the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)$ hence amounts to figuring out the multiplicity of each character of A in the representation $g \mapsto g^*$ of A in $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)$; it is the aim of this §3. The choice, in §3.1, of an isomorphism between $\boldsymbol{\mu}_n(\mathbb{F}_q)$ and $\boldsymbol{\mu}_n(\overline{\mathbb{Q}}_\ell)$ allows to identify $\hat{A}$ to the group of characters of A taking values in $\overline{\mathbb{Q}}_\ell$. After determining the character of the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$ in §3.2, we will prove in §3.3 that the multiplicity of $a \in \hat{A}$ is $m_a = \#(\mathbb{Z}/n\mathbb{Z} \setminus \{a_1, \ldots, a_n\})$.

3.1 Characters of A with values in $\overline{\mathbb{Q}}_\ell$

As we only consider the case $q \equiv 1 \mod n$, the group $\boldsymbol{\mu}_n(\mathbb{F}_q)$ consisting of the n^{th} roots of unity of $\mathbb{F}_q$ is isomorphic to the group of n^{th} roots of unity of $\overline{\mathbb{Q}}_\ell$. We call t an isomorphism of $\boldsymbol{\mu}_n(\mathbb{F}_q)$ onto $\boldsymbol{\mu}_n(\overline{\mathbb{Q}}_\ell)$ and use it to identify the group $\hat{A}$ with the group of characters of A taking values in $\overline{\mathbb{Q}}_\ell$ thanks to the isomorphism $[a_1, \ldots, a_n] \mapsto ([\zeta_1, \ldots, \zeta_n] \mapsto t(\zeta_1)^{a_1} \cdots t(\zeta_n)^{a_n})$.

3.2 Character values of the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathbf{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathbf{prim}}$

As p is prime to n by assumption, the elements of A have an order prime to p; we may thus use Formula (2.1) to obtain the values taken by the characters of the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$.

Theorem 3.1. *Consider $(\zeta_1, \ldots, \zeta_n) \in \boldsymbol{\mu}_n(\mathbb{F}_q)^n$ such that $\zeta_1 \ldots \zeta_n = 1$ and let g be the corresponding element $[\zeta_1, \ldots, \zeta_n]$ of A. For all $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$, denote by $k(\zeta)$ the number of $i \in [\![1; n]\!]$ such that $\zeta_i = \zeta$. We have*

$$\operatorname{tr}(g^* | H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) = \frac{(-1)^n}{n} \sum_{\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)} (1-n)^{k(\zeta)}. \tag{3.1}$$

Proof. A point of $\overline{X}_\psi$ with homogeneous coordinates $[x_1 : \ldots : x_n]$ is a fixed point of g if and only if $(x_1, \ldots, x_n)$ is proportional to $(\zeta_1 x_1, \ldots, \zeta_n x_n)$. The proportionality coefficient is necessarily a root of unity $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$, and we must have $x_i = 0$ if $\zeta_i \neq \zeta$. Hence, the subscheme of fixed points of g of $\overline{X}_\psi$ is the disjoint union over $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$ of the subvarieties

$$Y_\zeta = \{x \in \overline{X}_\psi \mid x_i = 0 \text{ if } \zeta_i \neq \zeta\}.$$

If $k(\zeta) = n$, we have $Y_\zeta = \overline{X}_\psi$. If $2 \leq k(\zeta) \leq n-1$, Y_ζ is isomorphic to the hypersurface of $\mathbb{P}^{k(\zeta)-1}$ defined by $y_1^n + y_2^n + \cdots + y_{k(\zeta)}^n = 0$. Finally, if $k(\zeta) = 0$ or 1, Y_ζ is empty. In each of these cases, we can apply Theorem 2.2 and obtain

$$\chi(Y_\zeta) = k(\zeta) - 1 + \frac{(1-n)^{k(\zeta)} + n - 1}{n} = k(\zeta) - \frac{1}{n} + \frac{(1-n)^{k(\zeta)}}{n}.$$

Consequently, since $\sum_{\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)} k(\zeta) = n$ and $\sum_{\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)} \frac{1}{n} = 1$,

$$\chi(\overline{X}_\psi^g) = \sum_{\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)} \chi(Y_\zeta) = n - 1 + \sum_{\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)} \frac{(1-n)^{k(\zeta)}}{n}.$$

Using trace formula (2.1) page 4, we deduce the announced result. $\square$

Remark 3.2. A recent preprint proves, in a more general setting, formulas of the type given in Theorem 3.1 and Theorem 4.12 page 10; see [Chênevert, 2009, Corollary 2.5].

3.3 Decomposition in irreducible representations

The following theorem gives a simple expression for the multiplicity m_a of a character $a \in \hat{A}$ in the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$.

Theorem 3.3. *The multiplicity of the irreducible character $a = [a_1, \ldots, a_n]$ of A in the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$ is*

$$m_a = \#(\mathbb{Z}/n\mathbb{Z} \setminus \{a_1, \ldots, a_n\}) = n - (\textit{number of distinct } a_i).$$

Proof. Consider $(\zeta_1, \ldots, \zeta_n) \in \boldsymbol{\mu}_n(\mathbb{F}_q)^n$ such that $\zeta_1 \ldots \zeta_n = 1$ and let g be the corresponding element $[\zeta_1, \ldots, \zeta_n]$ of A. From the definition, we have

$$\begin{aligned}\operatorname{tr}(g^* | H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) &= \sum_{a \in \hat{A}} m_a \zeta_1^{a_1} \ldots \zeta_n^{a_n} \\ &= \frac{1}{n} \sum_{\substack{(a_1, \ldots, a_n) \in (\mathbb{Z}/n\mathbb{Z})^n \\ a_1 + \cdots + a_n = 0}} m_a \zeta_1^{a_1} \ldots \zeta_n^{a_n}.\end{aligned}$$

We will show that if we replace m_a by the number of elements of $\mathbb{Z}/n\mathbb{Z} \setminus \{a_1, \dots, a_n\}$ in the right hand side, we recover Formula (3.1) above, which will show the announced result. We write

$$\begin{aligned}
&\frac{1}{n} \sum_{\substack{(a_1,\dots,a_n)\in(\mathbb{Z}/n\mathbb{Z})^n \\ a_1+\dots+a_n=0}} \#(\mathbb{Z}/n\mathbb{Z} \setminus \{a_1, \dots, a_n\}) \zeta_1^{a_1} \dots \zeta_n^{a_n} \\
&\qquad = \frac{1}{n} \sum_{\substack{(a_1,\dots,a_n)\in(\mathbb{Z}/n\mathbb{Z})^n \\ a_1+\dots+a_n=0}} \Bigg(\sum_{\substack{k\in\mathbb{Z}/n\mathbb{Z} \\ \forall i,\ a_i \neq k}} 1 \Bigg) \zeta_1^{a_1} \dots \zeta_n^{a_n} \\
&\qquad = \frac{1}{n} \sum_{k\in\mathbb{Z}/n\mathbb{Z}} \sum_{\substack{(a_1,\dots,a_n)\in(\mathbb{Z}/n\mathbb{Z})^n \\ a_1+\dots+a_n=0 \\ \forall i,\ a_i\neq k}} \zeta_1^{a_1} \dots \zeta_n^{a_n} \\
&\qquad = \frac{1}{n} \sum_{k\in\mathbb{Z}/n\mathbb{Z}} \sum_{\substack{(a_1,\dots,a_n)\in(\mathbb{Z}/n\mathbb{Z})^n \\ a_1+\dots+a_n=0 \\ \forall i,\ a_i\neq 0}} \zeta_1^{a_1} \dots \zeta_n^{a_n} \\
&\qquad = \sum_{\substack{(a_1,\dots,a_n)\in(\mathbb{Z}/n\mathbb{Z})^n \\ a_1+\dots+a_n=0 \\ \forall i,\ a_i\neq 0}} \zeta_1^{a_1} \dots \zeta_n^{a_n} \\
&\qquad = \sum_{\substack{a_1,\dots,a_n\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\} \\ a_1+\dots+a_n=0}} \zeta_1^{a_1} \dots \zeta_n^{a_n}.
\end{aligned}$$

We now conclude by using the following lemma. ☐

Lemma 3.4. *Let r be an integer ≥ 1 and $\zeta_1, \dots, \zeta_r$ elements of $\boldsymbol{\mu}_n(\mathbb{F}_q)$. If $k(\zeta) = k_{(\zeta_1,\dots,\zeta_r)}(\zeta)$ denotes the number of $i \in [\![1; r]\!]$ such that $\zeta_i = \zeta$, then*

$$\sum_{\substack{a_1,\dots,a_r\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\} \\ a_1+\dots+a_r=0}} \zeta_1^{a_1} \dots \zeta_r^{a_r} = \frac{(-1)^r}{n} \sum_{\zeta\in\boldsymbol{\mu}_n(\mathbb{F}_q)} (1-n)^{k(\zeta)}.$$

Proof. We proceed by induction on r. For $r = 1$, the equality is the relation

$$0 = -\frac{1}{n}\Big((1-n)^1 + (n-1)(1-n)^0\Big).$$

We now assume that $r \geq 2$ and that the result is known for $r-1$. We write

$$\begin{aligned}
\sum_{\substack{a_1,\dots,a_r\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\} \\ a_1+\dots+a_r=0}} \zeta_1^{a_1} \dots \zeta_r^{a_r} &= \sum_{\substack{a_1,\dots,a_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\} \\ a_1+\dots+a_{r-1}\neq 0}} \zeta_1^{a_1} \dots \zeta_{r-1}^{a_{r-1}} \zeta_r^{-a_1-\dots-a_{r-1}} \\
&= \sum_{a_1,\dots,a_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}} \left(\frac{\zeta_1}{\zeta_r}\right)^{a_1} \dots \left(\frac{\zeta_{r-1}}{\zeta_r}\right)^{a_{r-1}} \\
&\qquad - \sum_{\substack{a_1,\dots,a_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\} \\ a_1+\dots+a_{r-1}=0}} \zeta_1^{a_1} \dots \zeta_{r-1}^{a_{r-1}}.
\end{aligned}$$

Given $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$, we have

$$\sum_{a\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}} \zeta^a = \begin{cases} -1 & \text{if } \zeta \neq 1, \\ n-1 & \text{if } \zeta = 1. \end{cases}$$

This little remark allows to compute the first sum:

$$\sum_{a_1,\ldots,a_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}} \left(\frac{\zeta_1}{\zeta_r}\right)^{a_1} \cdots \left(\frac{\zeta_{r-1}}{\zeta_r}\right)^{a_{r-1}} = (-1)^{r-k(\zeta_r)}(n-1)^{k(\zeta_r)-1},$$

where $k(\zeta) = k_{(\zeta_1,\ldots,\zeta_r)}(\zeta)$. To compute the second sum, we use the induction assumption:

$$\sum_{\substack{a_1,\ldots,a_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ a_1+\cdots+a_{r-1}=0}} \zeta_1^{a_1}\cdots\zeta_{r-1}^{a_{r-1}} = \frac{(-1)^{r-1}}{n}\Bigg(\sum_{\zeta\neq\zeta_r}(1-n)^{k(\zeta)} + (1-n)^{k(\zeta_r)-1}\Bigg).$$

We conclude by noting that

$$\begin{aligned}&(-1)^{r-k(\zeta_r)}(n-1)^{k(\zeta_r)-1} - \frac{(-1)^{r-1}}{n}(1-n)^{k(\zeta_r)-1}\\ &\quad= -\frac{(-1)^r n(1-n)^{k(\zeta_r)-1}}{n} + \frac{(-1)^r}{n}(1-n)^{k(\zeta_r)-1} = \frac{(-1)^r}{n}(1-n)^{k(\zeta_r)}.\end{aligned}$$ □

Remark 3.5. As a consequence of Theorem 3.3, the multiplicity m_a of the character $a \in \hat{A}$ is nonzero unless a belongs to the orbit of $[0,1,2,\ldots,n-1]$ under $\mathfrak{S}_n$ (which imposes n odd, or else $1+2+\cdots+(n-1)$ is not divisible by n).

4 Action of G on $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$

4.1 A decomposition of the $\overline{\mathbb{Q}}_\ell[G]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$

For every a belonging to $\hat{A}$ identified to the group of characters of A taking values in $\overline{\mathbb{Q}}_\ell$, we denote by $\overline{H}_a$ the isotypic component relatively to a of the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$ (see [Bourbaki, 1958, §3.4]). It is a $\overline{\mathbb{Q}}_\ell$-vector space of dimension m_a, where m_a is the multiplicity computed in §3.3, and we have

$$H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}} = \bigoplus_{a\in\hat{A}} \overline{H}_a.$$

The group G acts on the left on A by inner automorphisms, and thus acts on the left on $\hat{A}$: if $g \in A\sigma$, with $\sigma \in \mathfrak{S}_n$, and if $a = [a_1,\ldots,a_n]$, we have ${}^g a = {}^\sigma a = [a_{\sigma^{-1}(1)},\ldots,a_{\sigma^{-1}(n)}]$.

Consider $a \in \hat{A}$. Denote by $\langle a\rangle$ the orbit of a under $\mathfrak{S}_n$. The stabilizer G_a of a in G is equal to $A \rtimes S_a$, where $S_a = \{\sigma \in \mathfrak{S}_n \mid {}^\sigma a = a\}$. We have $g\overline{H}_a = \overline{H}_{{}^g a}$ for all $g \in G$ and the space $\overline{H}_a$ is stable by G_a. The subspace $\bigoplus_{a'\in\langle a\rangle} \overline{H}_{a'}$ of $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$ is stable by G; it is a $\overline{\mathbb{Q}}_\ell[G]$-module canonically isomorphic to $\mathrm{Ind}_{G_a}^G \overline{H}_a$. We thus deduce the following result.

Theorem 4.1. *Denote by $R \subset \hat{A}$ a set of representatives of $\mathfrak{S}_n\backslash\hat{A}$. The $\overline{\mathbb{Q}}_\ell[G]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$ is isomorphic to*

$$\bigoplus_{a\in R} \mathrm{Ind}_{G_a}^G \overline{H}_a.$$

The aim of the rest of this §4 is to determine how the group S_a acts on $\overline{H}_a$. The strategy is the following: after showing that S_a is a semi-direct product $S'_a \rtimes \overline{\Sigma}_a$ (§4.2), we compute $\mathrm{tr}(\sigma^* | H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}})$ for σ a generator of S'_a and compare it to the trace of the identity (§4.4) to deduce that S'_a acts as $\epsilon(\sigma)\,\mathrm{Id}_{\overline{H}_a}$ on $\overline{H}_a$ (see §4.5). We then show, using a method similar to §3, that $\overline{\Sigma}_a$ acts as a multiple of the regular representation (§4.6–4.8).

The approach we use to study the action of S'_a is the same that Brünjes used in [Brünjes, 2004, Proposition 11.5, page 197] for the case $\psi = 0$, the only difference being that our trace formula allows us to avoid a tedious proof by induction.

4.2 Structure of S_a

Consider $a = [a_1, \dots, a_n] \in \hat{A}$, where $(a_1, \dots, a_n)$ is an element of $(\mathbb{Z}/n\mathbb{Z})^n$ such that $a_1+\cdots+a_n = 0$. The set of $j \in \mathbb{Z}/n\mathbb{Z}$ such that $(a_1 + j, \dots, a_n + j)$ is a permutation of $(a_1, \dots, a_n)$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$; it can be written as $n'_a\mathbb{Z}/n\mathbb{Z}$ for some integer $n'_a \geq 1$ dividing n; let $d_a = n/n'_a$ be the order of this group. These two integers only depend on a and not on the choice of $a_1, \dots, a_n$.

Remark 4.2. For all $b \in \mathbb{Z}/n\mathbb{Z}$, denote by $I(b)$ the set of $i \in \{1, \dots, n\}$ such that $a_i = b$. The set $n'_a\mathbb{Z}/n\mathbb{Z}$ is the set of $j \in \mathbb{Z}/n\mathbb{Z}$ such that $I(b + j)$ has the same number of elements as $I(b)$ for all $b \in \mathbb{Z}/n\mathbb{Z}$.

Lemma 4.3. *There is a permutation $\sigma \in \mathfrak{S}_n$ such that*

a) if $1 \leq i \leq n$, we have $a_{\sigma(i)} = a_i + n'_a$;

b) σ is the product of n'_a disjoint cycles of length d_a.

Proof. Let us note that the condition 4.3.a is equivalent to the fact that $\sigma(I(b)) = I(b+n'_a)$. For all $b \in \mathbb{Z}/n\mathbb{Z}$ such that $I(b) \neq \varnothing$, choose a numbering $i_1(b), \dots, i_{\#I(b)}(b)$ of the elements of $I(b)$ and denote by σ the element of $\mathfrak{S}_n$ which sends $i_l(b)$ to $i_l(b + n'_a)$ for all $b \in \mathbb{Z}/n\mathbb{Z}$ and $1 \leq l \leq \#I(b)$.

From the definition, we have $a_{\sigma(i)} = a_i + n'_a$ and, inspecting the orbits of each of the a_i under $b \mapsto b + n'_a$, we see that σ is a product of n'_a disjoint cycles of length d_a. □

Denote by S'_a the fixator of $(a_1, \dots, a_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ in $\mathfrak{S}_n$; it is a group which can be identified with $\prod_{b\in\mathbb{Z}/n\mathbb{Z}} \mathfrak{S}_{I(b)}$ (it is hence generated by transpositions) and we set $\gamma_a = [\mathfrak{S}_n : S'_a]$. Consider $\sigma \in \mathfrak{S}_n$ satisfying the conditions of the preceding lemma and let $\overline{\Sigma}_a = \langle\sigma\rangle$ be the cyclic subgroup of order d_a of $\mathfrak{S}_n$ generated by σ.

Proposition 4.4. *The fixator S_a of $a = [a_1, \dots, a_n] \in \hat{A}$ can be written as the semi-direct product*

$$S_a = S'_a \rtimes \overline{\Sigma}_a.$$

Proof. If $s \in S_a$, there exists a unique $j \in n'_a\mathbb{Z}/n\mathbb{Z}$ such that ${}^s(a_1, \dots, a_n) = (a_1 + j, \dots, a_n + j)$. This element only depends on a, not on the choice of $a_1, \dots, a_n$; we denote it by $j_a(s)$. The map $j_a\colon S_a \to n'_a\mathbb{Z}/n\mathbb{Z}$ thus defined is a group homomorphism. This homomorphism is surjective and its kernel is the fixator S'_a of $(a_1, \dots, a_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ in $\mathfrak{S}_n$.

Moreover, as $a_{\sigma(i)} = a_i + n'_a$ and thus $a_{\sigma^{-1}(i)} = a_i - n'_a$, we have $j_a(\sigma) = -n'_a$ by construction, hence j_a induces an isomorphism of $\overline{\Sigma}_a = \langle\sigma\rangle$ onto the image $n'_a\mathbb{Z}/n\mathbb{Z}$ of j_a, which shows that

$$S_a = S'_a \rtimes \overline{\Sigma}_a.$$ □

Remarks 4.5. *a)* In particular, the group S'_a is a normal subgroup of S_a and the quotient group S_a/S'_a is isomorphic to $n'_a\mathbb{Z}/n\mathbb{Z}$ and hence of order d_a.

b) Let us insist on the fact that n'_a, d_a, S'_a and j_a only depend on a and not on the choice of the representative $(a_1, \dots, a_n) \in \mathbb{Z}/n\mathbb{Z}$. The group $\overline{\Sigma}_a$ also only depends on a, but its construction is not canonical as it depends on an arbitrary choice of numbering.

c) Let us also note that if $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $d_{ka} = d_a$, $n'_{ka} = n'_a$, $S'_{ka} = S'_a$ and $S_{ka} = S_a$, but $j_{ka} = kj_a$.

4.3 Character values on a transposition τ

Theorem 4.6. *For any transposition $\tau \in \mathfrak{S}_n$, we have*

$$\operatorname{tr}(\tau^*|H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) = (-1)^n \left(\frac{(1-n)^{n-1} + (n-1)}{n} - \delta_n\right), \tag{4.1}$$

where, as previously, $\delta_n = 0$ if n is odd and $\delta_n = 1$ if n is even.

Proof. We may assume that $\tau = (1,2)$. We look for the fixed points of τ, i.e. the set of points $[x_1 : \ldots : x_n]$ such that $[x_1 : x_2 : x_3 : \ldots : x_n] = [x_2 : x_1 : x_3 : \ldots : x_n]$ and $x_1^n + \cdots + x_n^n - n\psi x_1 \ldots x_n = 0$. For such a point, we have $x_1^2 = x_2^2$, so that we are in one of the following two cases.

a) We have $x_1 = x_2$ and $2x_2^n + x_3^n + \cdots + x_n^n - n\psi x_2^2 x_3 \ldots x_n = 0$. The hypersurface of $\mathbb{P}^{n-2}$ defined by this equation is smooth because $\psi^n \neq 1$ and its Euler–Poincaré characteristic is $(n-2) + \frac{1}{n}[(1-n)^{n-1} + (n-1)]$ (Theorem 2.2).

b) We have $x_1 = -x_2 \neq 0$, in which case $x_3 = \cdots = x_n = 0$ and $x_1^n + x_2^n = 0$. This can only happen if n is odd and $[x_1 : \ldots : x_n] = [1 : -1 : 0 : \ldots : 0]$.

The Euler–Poincaré characteristic of the fixed-point subvariety of τ of $\overline{X}_\psi$ is thus

$$\begin{aligned}\chi(X_\psi^\tau) &= (n-2) + \frac{(1-n)^{n-1} + (n-1)}{n} + 1 - \delta_n \\ &= (n-1) + \frac{(1-n)^{n-1} + (n-1)}{n} - \delta_n,\end{aligned}$$

and consequently, as τ is of order 2 and $\mathbb{F}_q$ is of characteristic $\neq 2$, Theorem 2.6 applies:

$$\begin{aligned}\operatorname{tr}(\tau^* | H_{\mathrm{et}}^{n-2}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) &= (-1)^{n-1}\Big((n-1) - \chi(\overline{X}_\psi^\tau)\Big) \\ &= (-1)^n \left(\frac{(1-n)^{n-1} + (n-1)}{n} - \delta_n\right).\end{aligned}$$

□

4.4 Sum of the dimensions of the spaces $\overline{H}_a$ for $a \in \hat{A}^\tau$

Proposition 4.7. *Let $\tau \in \mathfrak{S}_n$ be a transposition. Denote by $\hat{A}^\tau$ the set of elements of $\hat{A}$ fixed by τ. We have*

$$\sum_{a \in \hat{A}^\tau} m_a = (-1)^{n-1}\left(\frac{(1-n)^{n-1} + (n-1)}{n} - \delta_n\right),$$

where, as previously, $\delta_n = 0$ if n is odd and $\delta_n = 1$ if n is even.

Proof. We may assume that $\tau = (1,2)$. Denote by B the set of elements $(b_1, \ldots, b_n) \in (\mathbb{Z}/n\mathbb{Z} \setminus \{0\})^n$ such that $b_1 = b_2$ and $b_1 + \cdots + b_n = 0$. The map $(b_1, \ldots, b_n) \mapsto [b_1, \ldots, b_n]$ from B to $\hat{A}^\tau$ is surjective and each element $a \in \hat{A}^\tau$ has exactly m_a elements in its preimage. We thus have $\sum_{a \in \hat{A}^\tau} m_a = \#B$ and conclude thanks to the following lemma. □

Lemma 4.8. *Let r be an integer ≥ 2. The number of r-uples $(b_1, \ldots, b_r)$ belonging to $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\})^r$ such that $b_1 = b_2$ and $b_1 + \cdots + b_r = 0$ is*

$$(-1)^{r-1}\left(\frac{(1-n)^{r-1} + (n-1)}{n} - \delta_n\right).$$

Proof. Denote by u_r the number we want to compute. We have $u_2 = \delta_n$ and $u_r + u_{r+1}$ is the number of $(r+1)$-uples $(b_1, \ldots, b_r, b_{r+1}) \in (\mathbb{Z}/n\mathbb{Z} \setminus \{0\})^r \times \mathbb{Z}/n\mathbb{Z}$ such that $b_1 = b_2$ and $b_1 + \cdots + b_{r+1} = 0$, that is, $u_r + u_{r+1} = (n-1)^{r-1}$. We deduce the announced result by induction on r. □

4.5 Action of S'_a on $\overline{H}_a$

We start with a general result on automorphisms of finite order with trace equal to the dimension of the space.

Lemma 4.9. *Let $\Bbbk$ be a field of characteristic zero, V a vector space of finite dimension over $\Bbbk$ and u an automorphism of V of finite order. If $\operatorname{tr} u = \dim V$, then $u = \mathrm{Id}_V$.*

Proof. Let M be the matrix of u in a certain basis of V over $\Bbbk$. The subfield $\Bbbk'$ of $\Bbbk$ generated by the coefficients of M embeds itself in $\mathbb{C}$; we can thus restrict ourselves to the case $\Bbbk = \mathbb{C}$.

Let $\lambda_1, \ldots, \lambda_m$ (where $m = \dim V$) be the (complex) eigenvalues of M, each repeated with multiplicity. They are all roots of unity. As we have, according to the assumptions of the lemma,

$$|\lambda_1 + \cdots + \lambda_m| = |\operatorname{tr} u| = m = |\lambda_1| + \cdots + |\lambda_m|,$$

the λ_i's are positively proportional, hence equal. As their sum is m, they are all equal to 1. The endomorphism u of V is thus unipotent; as it is of finite order, it is equal to Id_V. □

Remark 4.10. Let $\Bbbk$ be a field having characteristic zero, and $(V_i)_{i\in I}$ a finite sequence of vector space of finite dimensions over $\Bbbk$. For each $i \in I$, let u_i be an automorphism of V_i of finite order. If $\sum_{i\in I} \operatorname{tr} u_i$ is equal to $\sum_{i\in I} \dim V_i$ (respectively to $-\sum_{i\in I} \dim V_i$), then $u_i = \mathrm{Id}_{V_i}$ (respectively $u_i = -\mathrm{Id}_{V_i}$) for all $i \in I$. This results from Lemma 4.9 applied to the automorphism u of $V = \bigoplus_{i\in I} V_i$ which is equal to u_i (respectively to $-u_i$) over V_i for all $i \in I$.

Let $\tau \in \mathfrak{S}_n$ be a transposition. As $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}} = \bigoplus_{a\in\hat{A}} \overline{H}_a$ and as τ^* sends $\overline{H}_a$ into $\overline{H}_{{}^\tau a}$, we have

$$\operatorname{tr}(\tau^*|H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) = \sum_{a\in\hat{A}^\tau} \operatorname{tr}(\tau^*|\overline{H}_a).$$

By Theorem 4.6 and Proposition 4.7, we also have

$$\operatorname{tr}(\tau^*|H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) = -\sum_{a\in\hat{A}^\tau} \dim \overline{H}_a.$$

We thus deduce from Remark 4.10 that, for each $a \in \hat{A}^\tau$, τ^* acts on $\overline{H}_a$ by $-\mathrm{Id}_{\overline{H}_a}$.

Theorem 4.11. *Consider $a \in \hat{A}$ and $\sigma \in S'_a$. If we denote by $\epsilon(\sigma)$ the signature of σ, we have*

$$\sigma^*|\overline{H}_a = \epsilon(\sigma)\,\mathrm{Id}_{\overline{H}_a}.$$

Proof. The subgroup S'_a of $\mathfrak{S}_n$ is generated by the transpositions τ satisfying ${}^\tau a = a$ (see §4.2) and we have just seen that $\tau^*|\overline{H}_a = -\mathrm{Id}_{\overline{H}_a} = \epsilon(\tau)\,\mathrm{Id}_{\overline{H}_a}$. □

4.6 Character values on $A\sigma$ where σ is a product of n' disjoint cycles of length d

Let n' and d be integers ≥ 1 such that $n'd = n$ and let $\sigma \in \mathfrak{S}_n$ be a product of n' disjoint cycles of length d. Let $\zeta_1, \ldots, \zeta_n$ be elements of $\boldsymbol{\mu}_n(\mathbb{F}_q)$ such that $\zeta_1 \ldots \zeta_n = 1$ and denote by g the element $[\zeta_1, \ldots, \zeta_n]\sigma$ of $G = A \rtimes \mathfrak{S}_n$. Let $O_1, \ldots, O_{n'}$ be the n' orbits of σ in $\{1, \ldots, n\}$ and, for each $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$, denote by $k(\zeta)$ the number of $j \in \{1, \ldots, n'\}$ such that $\prod_{i\in O_j} \zeta_i = \zeta$. The following theorem generalizes Theorem 3.1 (which is recovered by taking $d = 1$ and $n' = n$ i.e. $\sigma = \mathrm{Id}$).

Theorem 4.12. *Under the preceding assumptions,*

$$\operatorname{tr}(g^*|H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) = \frac{(-1)^n}{n'} \sum_{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)} (1-n)^{k(\zeta)}.$$

Proof. We may assume that σ is the product of $((j-1)d+1, \ldots, jd)$ for $1 \leq j \leq n'$ and that $O_j = \{(j-1)d+1, \ldots, jd\}$. The fixed points of g in $X_\psi(\overline{\mathbb{F}}_q)$ are the points $[x_1 : \ldots : x_n]$ of $X_\psi(\overline{\mathbb{F}}_q)$ such that

$$[\zeta_{\sigma^{-1}(1)} x_{\sigma^{-1}(1)} : \ldots : \zeta_{\sigma^{-1}(n)} x_{\sigma^{-1}(n)}] = [x_1 : \ldots : x_n]$$

i.e.

$$[\zeta_1 x_1 : \ldots : \zeta_n x_n] = [x_{\sigma(1)} : \ldots : x_{\sigma(n)}].$$

The subscheme $\overline{X}_\psi^g$ of these fixed points is thus the disjoint union, over $\lambda \in \overline{\mathbb{F}}_q^*$, of the closed subschemes Y_λ of $\overline{X}_\psi$ defined by

$$(Y_\lambda) \qquad \begin{cases} x_1^n + \cdots + x_n^n - n\psi x_1 \ldots x_n = 0, \\ x_{\sigma(i)} = \lambda\zeta_i x_i \quad \text{for } 1 \le i \le n. \end{cases}$$

Let $j \in \{1, \ldots, n'\}$. If $\prod_{i \in O_j} \zeta_i \neq \lambda^{-d}$, the second relation shows that $x_i = 0$ for all $i \in O_j$. If $\prod_{i \in O_j} \zeta_i = \lambda^{-d}$, we have $\lambda \in \boldsymbol{\mu}_{nd}(\overline{\mathbb{F}}_q)$ and the second relation shows that

$$\sum_{i \in O_j} x_i^n = x_{jd}^n \left(\sum_{i=1}^{d} (\lambda^n)^i \right) = \begin{cases} d x_{jd}^n & \text{if } \lambda \in \boldsymbol{\mu}_n(\mathbb{F}_q), \\ 0 & \text{if } \lambda \notin \boldsymbol{\mu}_n(\mathbb{F}_q). \end{cases}$$

Consider $\lambda \in \overline{\mathbb{F}}_q^*$ and let $\zeta = \lambda^{-d}$ (as $n = n'd$, we have $\zeta^{n'} = 1 \iff \lambda^n = 1$). Denote by J the set of $j \in \{1, \ldots, n'\}$ such that $\prod_{i \in O_j} \zeta_i = \zeta$ and let $y_j = x_{jd}$ for each $j \in J$. If $\zeta \notin \boldsymbol{\mu}_n(\mathbb{F}_q)$, J is empty and hence Y_λ is empty. Assume now that $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$. The number of elements of J is $k(\zeta)$. We consider two cases.

a) First case: $\zeta \in \boldsymbol{\mu}_{n'}(\mathbb{F}_q)$. According to what we have just done, the scheme Y_λ is isomorphic to the hypersurface of $\mathbb{P}^{k(\zeta)-1}_{\overline{\mathbb{F}}_q}$ defined by

$$\begin{aligned} &d\left(\sum_{j \in J} y_j^n\right) = 0 \quad \text{if } J \neq \{1, \ldots, n'\}, \\ &d(y_1^n + \cdots + y_{n'}^n) - n\psi' y_1^d \ldots y_{n'}^d = 0 \quad \text{if } J = \{1, \ldots, n'\}, \end{aligned}$$

where ψ' is the product of ψ by an element of $\boldsymbol{\mu}_n(\overline{\mathbb{F}}_q)$. This hypersurface is smooth (because, in the second case, we have $(\psi')^n = \psi^n \neq 1$ and thus $(\psi')^{n'} \neq 1$), hence, by Theorem 2.2 page 3, we have

$$\chi(Y_\lambda) = k(\zeta) - 1 + \frac{(1-n)^{k(\zeta)} + (n-1)}{n} = k(\zeta) + \frac{(1-n)^{k(\zeta)} - 1}{n}.$$

b) Second case: $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q) \setminus \boldsymbol{\mu}_{n'}(\mathbb{F}_q)$. This time, the scheme Y_λ is isomorphic to $\mathbb{P}^{k(\zeta)-1}_{\overline{\mathbb{F}}_q}$ if $J \neq \{1, \ldots, n'\}$ and to the hypersurface of $\mathbb{P}^{n'-1}_{\overline{\mathbb{F}}_q}$ defined by $(y_1 \ldots y_{n'})^d = 0$ if $J = \{1, \ldots, n'\}$. In the first case, we have $\chi(Y_\lambda) = k(\zeta)$. In the second case, we necessarily have $n' \geq 2$ and the Euler–Poincaré characteristic of Y_λ is equal to that of Y_λ^{red}, which is the union in $\mathbb{P}^{n'-1}_{\overline{\mathbb{F}}_q}$ of the hyperplanes defined by $y_j = 0$, hence

$$\begin{aligned} \chi(Y_\lambda) &= \sum_{\substack{L \subset \{1, \ldots, n'\} \\ L \neq \varnothing}} (-1)^{\#L - 1}(n' - \#L) = \sum_{l=1}^{n'} (-1)^{l-1} \binom{n'}{l} (n' - l) \\ &= n' \sum_{l=1}^{n'-1} (-1)^{l-1} \binom{n'-1}{l} = n'(1 - (1 + (-1))^{n'-1}) = n' = k(\zeta). \end{aligned}$$

For each $\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)$, there exists exactly d values of λ such that $\lambda^{-d} = \zeta$. Thus

$$\begin{aligned} \chi(\overline{X}_\psi^g) &= \sum_{\lambda \in \overline{\mathbb{F}}_q^*} \chi(Y_\lambda) = d \sum_{\zeta \in \boldsymbol{\mu}_n(\mathbb{F}_q)} k(\zeta) + d \sum_{\zeta \in \boldsymbol{\mu}_{n'}(\mathbb{F}_q)} \frac{(1-n)^{k(\zeta)} - 1}{n} \\ &= dn' + \sum_{\zeta \in \boldsymbol{\mu}_{n'}(\mathbb{F}_q)} \frac{(1-n)^{k(\zeta)} - 1}{n'} = n - 1 + \sum_{\zeta \in \boldsymbol{\mu}_{n'}(\mathbb{F}_q)} \frac{(1-n)^{k(\zeta)}}{n'}. \end{aligned}$$

The order of g divides nd and hence is prime to q; thus, by Theorem 2.6,

$$\begin{aligned}\operatorname{tr}(g^*|H^{n-2}_{\text{et}}(\overline{X}_\psi,\overline{\mathbb{Q}}_\ell)^{\text{prim}}) &= (-1)^{n-1}\Big((n-1)-\chi(\overline{X}^g_\psi)\Big)\\ &= \frac{(-1)^n}{n'}\sum_{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)}(1-n)^{k(\zeta)}.\end{aligned}$$

□

4.7 Trace of a product σ of n' disjoint cycles of length d acting on $\overline{H}_a$ when $a\in\hat{A}^\sigma$

We keep the notations of §4.6.

Lemma 4.13. *If $\sigma\in\mathfrak{S}_n$ is a product of n' disjoint cycles of length d,*

$$\sum_{a\in\hat{A}\text{ such that }\sigma\in S_{\bar{a}'}} a(\zeta_1,\ldots,\zeta_n)m_a = \frac{(-1)^{n'}}{n'}\sum_{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)}(1-n)^{k(\zeta)}.$$

Proof. Denote by B the set of $(b_1,\ldots,b_n)\in((\mathbb{Z}/n\mathbb{Z})\setminus\{0\})^n$ such that $b_1+\cdots+b_n=0$ and ${}^\sigma(b_1,\ldots,b_n)=(b_1,\ldots,b_n)$. The image of the map $B\to\hat{A}$, $(b_1,\ldots,b_n)\mapsto[b_1,\ldots,b_n]$ is the set of $a\in\hat{A}$ such that $\sigma\in S'_a$; such an element a has exactly m_a elements in its preimage. The sum we must compute can hence be rewritten as

$$\sum_{(b_1,\ldots,b_n)\in B}\zeta_1^{b_1}\ldots\zeta_n^{b_n}.$$

If $(b_1,\ldots,b_n)\in B$, all the b_i, for i belonging to an orbit O_j of σ, are equal to a common $c_j\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}$ and we have $d(c_1+\ldots c_{n'})=0$ in $\mathbb{Z}/n\mathbb{Z}$ i.e. $c_1+\cdots+c_{n'}\in n'\mathbb{Z}/n\mathbb{Z}$. Our sum can thus be rewritten as

$$\sum_{\substack{c_1,\ldots,c_{n'}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ c_1+\cdots+c_{n'}\in n'\mathbb{Z}/n\mathbb{Z}}}\mu_1^{c_1}\ldots\mu_{n'}^{c_{n'}},$$

where $\mu_j=\prod_{i\in O_j}\zeta_i$. We conclude by using the following generalization of Lemma 3.4 (which is recovered by taking $d=1$ and $n'=n$ i.e. $\sigma=\mathrm{Id}$). □

Lemma 4.14. *Let r be an integer ≥ 1 and $\mu_1,\ \ldots,\ \mu_r$ elements of $\boldsymbol{\mu}_n(\mathbb{F}_q)$. For each $\zeta\in\boldsymbol{\mu}_n(\mathbb{F}_q)$, we denote by $k(\zeta)$ the number of $j\in\{1,\ldots,r\}$ such that $\mu_j=\zeta$. We have*

$$\sum_{\substack{c_1,\ldots,c_r\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ c_1+\cdots+c_r\in n'\mathbb{Z}/n\mathbb{Z}}}\mu_1^{c_1}\ldots\mu_r^{c_r}=\frac{(-1)^r}{n'}\sum_{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)}(1-n)^{k(\zeta)}.$$

Proof. We prove the result by induction on r. For $r=1$, we have

$$\sum_{c_1\in n'\mathbb{Z}/n\mathbb{Z}\setminus\{0\}}\mu_1^{c_1}=\begin{cases}d-1=\frac{-1}{n'}((1-n)^1+(n'-1)(1-n)^0) & \text{if }\mu_1\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q),\\ -1=\frac{-1}{n'}(n'(1-n)^0) & \text{if }\mu_1\notin\boldsymbol{\mu}_{n'}(\mathbb{F}_q),\end{cases}$$

hence the result in that case. Assume now that $r\geq 2$ and that the result is proved for $r-1$. We write

$$
\begin{aligned}
&\sum_{\substack{c_1,\dots,c_r\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ c_1+\dots+c_r\in n'\mathbb{Z}/n\mathbb{Z}}} \mu_1^{c_1}\dots\mu_r^{c_r} + \sum_{\substack{c_1,\dots,c_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ c_1+\dots+c_{r-1}\in n'\mathbb{Z}/n\mathbb{Z}}} \mu_1^{c_1}\dots\mu_{r-1}^{c_{r-1}}\\
&\quad= \sum_{\substack{c_1,\dots,c_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ c_r\in\mathbb{Z}/n\mathbb{Z}\\ c_1+\dots+c_r\in n'\mathbb{Z}/n\mathbb{Z}}} \mu_1^{c_1}\dots\mu_r^{c_r}\\
&\quad= \sum_{\substack{c_1,\dots,c_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ l\in n'\mathbb{Z}/n\mathbb{Z}}} \mu_1^{c_1}\dots\mu_{r-1}^{c_{r-1}}\mu_r^{l-c_1-\dots-c_{r-1}}\\
&\quad= \sum_{c_1,\dots,c_{r-1}\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}} \left(\frac{\mu_1}{\mu_r}\right)^{c_1}\dots\left(\frac{\mu_{r-1}}{\mu_r}\right)^{c_{r-1}} \sum_{l\in n'\mathbb{Z}/n\mathbb{Z}} \mu_r^l.
\end{aligned}
$$

The sum $\sum_{l\in n'\mathbb{Z}/n\mathbb{Z}}\mu_r^l$ is equal to d if $\mu_r\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)$ and to 0 otherwise whereas $\sum_{c_i\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}}(\frac{\mu_i}{\mu_r})^{c_i}$ is equal to $n-1$ if $\mu_i=\mu_r$ and to -1 otherwise. The product of all these sums is thus equal to $(-1)^{r-1}d(1-n)^{k(\mu_r)-1}$ if $\mu_r\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)$ and to 0 otherwise.

Taking into account the induction assumption, we obtain

$$
\begin{aligned}
&\sum_{\substack{c_1,\dots,c_r\in(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}\\ c_1+\dots+c_r\in n'\mathbb{Z}/n\mathbb{Z}}} \mu_1^{c_1}\dots\mu_r^{c_r}\\
&\quad= \sum_{\substack{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)\\ \zeta\neq\mu_r}} (-1)^r\frac{(1-n)^{k(\zeta)}}{n'}\\
&\qquad\qquad + \sum_{\substack{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)\\ \zeta=\mu_r}} \left((-1)^r\frac{(1-n)^{k(\zeta)-1}}{n'} - d(-1)^r(1-n)^{k(\zeta)-1}\right)\\
&\quad= \frac{(-1)^r}{n'}\sum_{\zeta\in\boldsymbol{\mu}_{n'}(\mathbb{F}_q)}(1-n)^{k(\zeta)}.
\end{aligned}
$$

□

Theorem 4.15. *If σ is a product of n' disjoint cycles of length d and if $a\in\hat{A}^\sigma$, then*

$$
\operatorname{tr}(\sigma^*|\overline{H}_a) = \begin{cases}(-1)^{n-n'}m_a & \text{if } \sigma\in S'_a,\\ 0 & \text{if } \sigma\in S_a\setminus S'_a.\end{cases}
$$

Proof. As $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi,\overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}=\bigoplus_{a\in\hat{A}}\overline{H}_a$ and as σ^* sends $\overline{H}_a$ into $\overline{H}_{\sigma a}$, we have, for each $(\zeta_1,\dots,\zeta_n)\in\boldsymbol{\mu}_n(\mathbb{F}_q)^n$ satisfying $\zeta_1\dots\zeta_n=1$,

$$
\operatorname{tr}(([\zeta_1,\dots,\zeta_n]\sigma)^*|H^{n-2}_{\mathrm{et}}(\overline{X}_\psi,\overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}) = \sum_{a\in\hat{A}^\sigma} a(\zeta_1,\dots,\zeta_n)\operatorname{tr}(\sigma^*|\overline{H}_a).
$$

Moreover, by Theorem 4.12 and Lemma 4.13,

$$
\sum_{a\in\hat{A}\text{ such that }\sigma\in S'_a}(-1)^{n-n'}m_a\,a(\zeta_1,\dots,\zeta_n) = \sum_{a\in\hat{A}^\sigma}\operatorname{tr}(\sigma^*|\overline{H}_a)\,a(\zeta_1,\dots,\zeta_n)
$$

As this is valid for all $(\zeta_1,\dots,\zeta_n)\in\boldsymbol{\mu}_n(\mathbb{F}_q)^n$ satisfying $\zeta_1\dots\zeta_n=1$, we may identify the coefficients, which gives the announced result. □

4.8 Action of S_a on $\overline{H}_a$

Let's recapitulate the results of §§4.3–4.7. We keep the notations of §4.2: $a = [a_1, \ldots, a_n]$ is an element of $\hat{A}$, $n'_a\mathbb{Z}/n\mathbb{Z}$ is the set of $j \in \mathbb{Z}/n\mathbb{Z}$ such that $(a_1 + j, \ldots, a_n + j)$ is a permutation of $(a_1, \ldots, a_n)$ and $d_a = n/n'_a$; the fixator S_a of a in $\mathfrak{S}_n$ can be written as

$$\begin{aligned} S_a = S'_a \rtimes \overline{\Sigma}_a \quad \text{where} \quad & S'_a \text{ is the fixator of } (a_1, \ldots, a_n) \text{ in } \mathfrak{S}_n, \\ \text{and} \quad & \overline{\Sigma}_a = \langle \sigma \rangle \text{ is a cyclic group of order } d_a, \end{aligned}$$

with σ a product of n'_a disjoint cycles of length d_a.

The dimension m_a of $\overline{H}_a$ is, by Theorem 3.3, equal to $\#(\mathbb{Z}/n\mathbb{Z} \setminus \{a_1, \ldots, a_n\})$. It is a multiple of d_a as $\{a_1, \ldots, a_n\}$ is stable by translation by elements of $n'_a\mathbb{Z}/n\mathbb{Z}$; we can thus write $m_a = d_a m'_a$.

Theorem 4.16. *The group S_a acts on $\overline{H}_a$ as follows:*

- *an element $s \in S'_a$ acts by $\epsilon(s)\,\mathrm{Id}_{\overline{H}_a}$;*
- *an element $s \in \overline{\Sigma}_a$ acts by m'_a copies of the regular representation of $\overline{\Sigma}_a$.*

Proof. The first assertion results from Theorem 4.11 and the second from Theorem 4.15: the trace of σ^i acting on $\overline{H}_a$ is zero if $1 \le i \le n-1$ and equal to $m_a = \dim \overline{H}_a$ if $i = 0$ (note that $(-1)^{n-n'_a} = 1$ since both n and n'_a are odd), hence $\overline{\Sigma}_a$ acts as $m'_a = m_a/d_a$ copies of the regular representation. □

This completely determines the structure of the $\overline{\mathbb{Q}}_\ell[S_a]$-module $\overline{H}_a$. From the considerations of §4.1, we deduce the structure of the $\overline{\mathbb{Q}}_\ell[G]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$:

$$H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}} \simeq \bigoplus_{a \in R} \mathrm{Ind}^G_{A \rtimes S_a}\,(a \otimes \epsilon \otimes \mathrm{reg}^{m'_a}_{S_a/S'_a}), \tag{4.2}$$

where reg_{S_a/S'_a} is the regular representation of S_a/S'_a (let us recall that $R \subset \hat{A}$ is a set of representative elements of $\mathfrak{S}_n \backslash \hat{A}$; see §4.1).

5 Action of G on $H^{n-2}_{\mathbf{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathbf{prim}}$

We begin by giving a canonical construction of cyclotomic fields and characters attached to cyclic groups.

5.1 The cyclotomic field attached to a cyclic group

Let C be a cyclic group of order $m \ge 1$. Denote by $\mathbb{Q}[C]$ the group algebra of C over $\mathbb{Q}$ and by $\mathfrak{m}_C$ the ideal of $\mathbb{Q}[C]$ generated by the sums $\sum_{x \in C'} [x]$ for C' a subgroup $\neq \{1\}$ of C.

Theorem 5.1. *The ideal $\mathfrak{m}_C$ of $\mathbb{Q}[C]$ is maximal and the field $\mathbb{K}_C = \mathbb{Q}[C]/\mathfrak{m}_C$ is isomorphic to the cyclotomic field $\mathbb{Q}(\boldsymbol{\mu}_m)$ of m^{th} roots of unity.*

Proof. We may assume that $C = \mathbb{Z}/m\mathbb{Z}$ so that the algebra $\mathbb{Q}[C]$ can be identified with $\mathbb{Q}[X]/(X^m - 1)\mathbb{Q}[X]$. We have $X^m - 1 = \prod_{d|m} \Phi_d$, where Φ_d is the d^{th} cyclotomic polynomial. The polynomials Φ_d are paiwise prime in $\mathbb{Q}[X]$. From the chinese remainder theorem, we deduce that $\mathbb{Q}[X]/(X^m - 1)\mathbb{Q}[X]$ is isomorphic to $\prod_{d|m} \mathbb{Q}[X]/\Phi_d\mathbb{Q}[X]$. We now proceed to show that $\mathfrak{m}_C$ is the kernel of the projection $\phi\colon \mathbb{Q}[X]/(X^m - 1)\mathbb{Q}[X] \to \mathbb{Q}[X]/\Phi_m\mathbb{Q}[X]$. Let $d \neq m$ be an integer dividing m and $C_d = d\mathbb{Z}/m\mathbb{Z}$ the unique subgroup of C with index d; the element $\sum_{x \in C_d} [x]$ of $\mathbb{Q}[C]$ has projection 0 on $\mathbb{Q}[X]/\Phi_m\mathbb{Q}[X]$ and projection $\neq 0$ (equal to m/d) on $\mathbb{Q}[X]/\Phi_d\mathbb{Q}[X]$, which shows the result. □

The field $\mathbb{K}_C$ is called *the cyclotomic field attached to the cyclic group C*. The compound map

$$C \to \mathbb{Q}[C] \to \mathbb{K}_C = \mathbb{Q}[C]/\mathfrak{m}_C$$

is a canonical character χ_C of C taking values in $\mathbb{K}_C$. It induces an isomorphism between C and the group of m^{th} roots of unity of $\mathbb{K}_C$.

Proposition 5.2. *The field $\mathbb{K}_C$ is a simple $\mathbb{Q}[C]$-module with endomorphism ring $\mathbb{K}_C$.*

Let C_1 and C_2 be two cyclic groups of same order m and $\phi\colon C_1 \to C_2$ and isomorphism of C_1 onto C_2. The homomorphism $\mathbb{Q}[C_1] \to \mathbb{Q}[C_2]$ extending ϕ factors as an isomorphism $\mathbb{K}_\phi\colon \mathbb{K}_{C_1} \to \mathbb{K}_{C_2}$ and we have $\mathbb{K}_\phi \circ \chi_{C_1} = \chi_{C_2} \circ \phi$, i.e. the following diagram is commutative

$$\begin{array}{ccc} C_1 & \xrightarrow{\phi} & C_2 \\ {\scriptstyle \chi_{C_1}}\big\downarrow & & \big\downarrow{\scriptstyle \chi_{C_2}} \\ \mathbb{K}_{C_1} & \xrightarrow{\mathbb{K}_\phi} & \mathbb{K}_{C_2} \end{array}$$

5.2 The simple $\mathbb{Q}[A]$-module attached to an element of $(\mathbb{Z}/n\mathbb{Z})^\times\backslash\hat{A}$

The group $(\mathbb{Z}/n\mathbb{Z})^\times$ acts on $\hat{A}$ by $k \times [a_1, \ldots, a_n] = [ka_1, \ldots, ka_n]$. If $a \in \hat{A}$, we denote by $\bar{a}$ the class mod $(\mathbb{Z}/n\mathbb{Z})^\times$ of a. Let us note that the integers d_a and n'_a defined in §4.2 only depend on $\bar{a}$ and not on a (see Remark 4.5).

Denote by n_a the order of a in the group $\hat{A}$; it only depends on $\bar{a}$ and not on a. If m is an integer, we have $ma = 0$ if and only if all the ma_i are equal, i.e. if and only if $m(a_i - a_{i'}) = 0$ for all i and i' between 1 and n. The subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by the elements $a_i - a_{i'}$ only depends on $\bar{a}$ and not on a or on the choice of $a_1, \ldots, a_n$; it can be written as $f_a\mathbb{Z}/n\mathbb{Z}$ where f_a divides n and its order is n_a, hence $n = n_a f_a$. The integer f_a only depends on $\bar{a}$, not on a.

Following §3.1, we identify the group $\hat{A}$ to the group of characters of A taking values in $\mathbb{F}_q$, the element $a \in \hat{A}$ corresponding to the character $[\zeta_1, \ldots, \zeta_n] \mapsto \zeta_1^{a_1} \ldots \zeta_n^{a_n}$. If N_a and E_a denote the kernel and the image of this character, $E_a \simeq A/N_a$ is a cyclic subgroup of order n_a. Let us note that E_a and N_a only depend on $\bar{a}$, not on a.

Denote by $\mathbb{K}_a$ the cyclotomic field attached to the cyclic group E_a (see §5.1) and χ_a the compound character

$$A \twoheadrightarrow A/N_a \xrightarrow{\sim} E_a \hookrightarrow \mathbb{K}_a,$$

where the third arrow is the canonical character of E_a from §5.1.

Remarks 5.3. *a*) Consider $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. We have $ka = a$ if and only if $k \equiv 1 \mod n_a\mathbb{Z}$.

b) The cyclotomic field $\mathbb{K}_a$ only depends on $\bar{a}$ and not on a, but $\chi_{ka} = \chi_a^k$.

Proposition 5.4. *The character χ_a defines a structure of simple $\mathbb{Q}[A]$-module on $\mathbb{K}_a$ whose endomorphism ring is canonically isomorphic to the field $\mathbb{K}_a$.*

5.3 The stabilizer $S_{\bar{a}}$ in $\mathfrak{S}_n$ of an element $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times\backslash\hat{A}$

The group $\mathfrak{S}_n$ acts on $\hat{A}$ by ${}^\sigma[a_1, \ldots, a_n] = [a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)}]$. This action commutes to that of $(\mathbb{Z}/n\mathbb{Z})^\times$ and factors as an action of $\mathfrak{S}_n$ on $(\mathbb{Z}/n\mathbb{Z})^\times\backslash\hat{A}$. We designate by $S_{\bar{a}}$ the fixator of $\bar{a}$ in $\mathfrak{S}_n$.

If $\sigma \in S_{\bar{a}}$, there exists a unique $k \in (\mathbb{Z}/n_a\mathbb{Z})^\times$ such that ${}^\sigma a = ka$; we denote it by $k_a(\sigma)$. The map $k_a\colon S_{\bar{a}} \to (\mathbb{Z}/n_a\mathbb{Z})^\times$ defined in that way is a group homomorphism which is not surjective in general[2]. Its kernel is the group S_a from §4.2; in particular, S_a is a normal subgroup of $S_{\bar{a}}$. Let us note that the map k_a only depends on $\bar{a}$, not on a.

[2]Consider $n = 5$ and $a = [0, 0, 1, 1, 3]$: we have $n_a = 5$, but there is no $\sigma \in \mathfrak{S}_5$ such that ${}^\sigma a = 2a$.

From the definition of n'_a, there is an i such that $a_1 = a_i + n'_a$, i.e. $n'_a = a_1 - a_i \in f_a\mathbb{Z}/n\mathbb{Z}$. Thus, there is an integer e_a such that $n'_a = e_a f_a$ and we have $n = d_a e_a f_a$ and $n_a = d_a e_a$. The integer e_a only depends on $\bar{a}$, not on a.

Theorem 5.5. *The image of the homomorphism $k_a\colon S_{\bar{a}} \to (\mathbb{Z}/n_a\mathbb{Z})^\times$ contains the elements of $(\mathbb{Z}/n_a\mathbb{Z})^\times$ which are $\equiv 1 \mod e_a$ and is thus the preimage of a subgroup of $(\mathbb{Z}/e_a\mathbb{Z})^\times$ by the canonical surjection $(\mathbb{Z}/n_a\mathbb{Z})^\times \to (\mathbb{Z}/e_a\mathbb{Z})^\times$.*

Proof. Given $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $k \equiv 1 \mod e_a$, we must find a permutation $\sigma \in \mathfrak{S}_n$ such that ${}^\sigma a = ka$. We only need to show that there exists j such that, for all $b \in \mathbb{Z}/n\mathbb{Z}$, the sets $I(kb+j)$ and $I(b)$ have the same number of elements. The following lemma shows that we may take $j = -ka_1 + a_1$. ☐

Lemma 5.6. *If $k \equiv 1 \mod e_a$, then, for all $b \in \mathbb{Z}/n\mathbb{Z}$, $I(kb - ka_1 + a_1)$ has the same number of elements as $I(b)$.*

Proof. Consider $b \in \mathbb{Z}/n\mathbb{Z}$. Suppose that $b \equiv a_1 \mod f_a$, so that $(kb - ka_1 + a_1) - b = (k-1)(b-a_1)$ is a multiple of $e_a f_a = n'_a$ and thus $kb - ka_1 + a_1 \equiv b \mod n'_a$; by Remark 4.2, this implies that $I(kb - ka_1 + a_1)$ has the same number of elements as $I(b)$.

Suppose now that $b \not\equiv a_1 \mod f_a$ (and thus $I(b) = \varnothing$); in that case, $kb - ka_1$ is non zero mod f_a and so, from the definition of f_a, $kb - ka_1 + a_1$ is not one of the a_i's, which shows that $I(kb - ka_1 + a_1)$ is empty. ☐

We now determine the structure of $S_{\bar{a}}$. Let us recall (see Remark 4.5) that S'_a and S_a depend only on $\bar{a}$, not on a.

Theorem 5.7. *The group S'_a is a normal subgroup of $S_{\bar{a}}$ and the following short exact sequence splits*

$$1 \to S'_a \to S_{\bar{a}} \to S_{\bar{a}}/S'_a \to 1.$$

Proof. From the definition of f_a, it is possible to choose the representative $(a_1, \ldots, a_n)$ of a in $(\mathbb{Z}/n\mathbb{Z})^n$ such that each a_i is a multiple of f_a; because $f_a n_a = n$, the elements wa_i and wf_a, where $w \in (\mathbb{Z}/n_a\mathbb{Z})^\times$, are well-defined in $\mathbb{Z}/n\mathbb{Z}$. If $\sigma \in S_{\bar{a}}$, there is a unique pair $(u_\sigma, v_\sigma) \in \mathbb{Z}/n_a\mathbb{Z} \times (\mathbb{Z}/n_a\mathbb{Z})^\times$ such that, for all i, we have $a_{\sigma(i)} = v_\sigma a_i + u_\sigma f_a$. The uniqueness of v_σ comes from the fact that, as we have already seen (Remark 5.3), a k such that $ka = {}^\sigma a$ is defined mod n_a and the uniqueness of u_σ comes from the fact that $u_\sigma f_a$ is unique mod n.

The map $\phi\colon \sigma \mapsto (u_\sigma, v_\sigma)$ is a group homomorphism from $S_{\bar{a}}$ to $\mathbb{Z}/n_a\mathbb{Z} \rtimes (\mathbb{Z}/n_a\mathbb{Z})^\times$ (the group law being $(u,v)(u',v') = (u + vu', vv')$); its kernel is S'_a which is thus a normal subgroup of $S_{\bar{a}}$.

For each $b \in \mathbb{Z}/n\mathbb{Z}$, we choose a numbering $i_1(b), \ldots, i_{\#I(b)}(b)$ of the elements of $I(b)$. Given $(u,v) \in \phi(S_{\bar{a}})$, if $I(b)$ is non-empty, then b is a multiple of f_a (by assumption) and $I(b)$ has the same number of elements than $I(vb + uf_a)$ as $a_{\sigma(i)} = va_i + uf_a$ for all $\sigma \in S_{\bar{a}}$ satisfying $\phi(\sigma) = (u,v)$. Thus, there is a permutation $\sigma_{u,v} \in \mathfrak{S}_n$ sending $i_l(b)$ on $i_l(vb + uf_a)$ for all $b \in \mathbb{Z}/n\mathbb{Z}$ and $1 \leq l \leq \#I(b)$. From its definition, this permutation belongs to $S_{\bar{a}}$ and $\phi(\sigma_{u,v}) = (u,v)$. Moreover, the map $(u,v) \mapsto \sigma_{u,v}$ is a group homomorphism since we have

$$v'(vb + uf_a) + u'f_a = (v'v)b + (u' + v'u)f_a.$$

This shows that $(u,v) \mapsto \sigma_{u,v}$ is a splitting map for ϕ and thus the short exact sequence $1 \to S'_a \to S_{\bar{a}} \to S_{\bar{a}}/S'_a \to 1$ splits. ☐

Remarks 5.8. *a*) Even though S_a is a normal subgroup of $S_{\bar{a}}$, the exact short sequence $1 \to S_a \to S_{\bar{a}} \to S_{\bar{a}}/S_a \to 1$ does not always splits. Indeed, consider the case $n = 24$ and the sequence $(a_1, \ldots, a_{24})$ with four times each of the numbers 0, 2, 12, 14 and two times each of the numbers 1, 7, 13, 19; we have $n_a = 24$, but, even though 5 is of order 2 in $(\mathbb{Z}/24\mathbb{Z})^\times$, the only elements (u,v) of the image of ϕ such that $v = 5$ are $(2,5)$ and $(14,5)$ which are of order 4.

b) When $\sigma \in S_a$, we have $v_\sigma = 1$ and $u_\sigma \in e_a\mathbb{Z}/n_a\mathbb{Z}$; indeed, if $\sigma \in S_a$, then $v_\sigma = 1$ and so $a_{\sigma(i)} - a_i = u_\sigma f_a$; thus, from the definition of n'_a, $u_\sigma f_a$ is a multiple of $n'_a = e_a f_a$ and hence u_σ is a multiple of e_a.

c) With the notations of §4.2, we have, for all $s \in S_a$, $j_a(s) = f_a u_s$. More precisely, $j_a\colon S_a \to n'_a\mathbb{Z}/n\mathbb{Z}$ is the compound of the homomorphism $\sigma \mapsto u_s$ sending S_a into $e_a\mathbb{Z}/n_a\mathbb{Z}$ and of the isomorphism of $e_a\mathbb{Z}/n_a\mathbb{Z}$ onto $n'_a\mathbb{Z}/n\mathbb{Z}$ deduced from the multiplication by f_a.

5.4 Construction of $\mathbb{Q}[G]$-modules and study of their extension of scalars to $\overline{\mathbb{Q}}_\ell$

The aim of this §5.4 is to construct $\mathbb{Q}[G]$-modules which, after extension of scalars to $\overline{\mathbb{Q}}_\ell$, will give back the representations considered in §4.

Before we begin, let us recall that the field $\mathbb{K}_a$ only depends on $\bar{a}$, not on a, but that $\chi_{ka} = \chi_a^k$ (see Remark 5.3). If $v \in (\mathbb{Z}/n_a\mathbb{Z})^\times$, we denote by θ_v the automorphism of the field $\mathbb{K}_a$ sending every ${n_a}^{\text{th}}$ root of unity onto its v^{th} power.

Consider $a \in \hat{A}$; we choose a representative $(a_1, \dots, a_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ of a such that the a_i are all multiple of f_a and continue to use the notations of §5.3 concerning the integers u_σ and v_σ.

Proposition 5.9. *If ω is a ${n_a}^{th}$ root of unity in $\mathbb{K}_a$, the following map defines a representation of $A \rtimes S_{\bar{a}}$ into $\mathbb{K}_a$*

$$\begin{aligned} \mu_{a,\omega} \ &: \ A \rtimes S_{\bar{a}} \to \operatorname{End}_{\mathbb{Q}}(\mathbb{K}_a) \\ &(\zeta, \sigma) \ \mapsto \chi_a(\zeta)\epsilon(\sigma)\omega^{u_\sigma}\theta_{v_\sigma} \end{aligned}$$

Let $M_{a,\omega}$ be the $\mathbb{Q}[A \rtimes S_{\bar{a}}]$-module $\mathbb{K}_a$ thus defined. It has rank $\phi(n_a)$ (where ϕ is Euler's totient function), and, up to isomorphism, it is independent of the choice of the representative $(a_1, \dots, a_n)$ of a such that each a_i is divisible by f_a.

Proof. Let us first check that $\mu_{a,\omega}$ is a group homomorphism. We have

$$\begin{aligned} \mu_{a,\omega}(\zeta,\sigma)\mu_{a,\omega}(\zeta',\sigma') &= \chi_a(\zeta)\epsilon(\sigma)\omega^{u_\sigma}\theta_{v_\sigma}\chi_a(\zeta')\epsilon(\sigma')\omega^{u_{\sigma'}}\theta_{v_{\sigma'}} \\ &= \chi_a(\zeta)\chi_a(\zeta')^{v_\sigma}\epsilon(\sigma)\epsilon(\sigma')\omega^{u_\sigma+u_{\sigma'}v_\sigma}\theta_{v_\sigma v_{\sigma'}}, \end{aligned}$$

and

$$\begin{aligned} \mu_{a,\omega}((\zeta,\sigma)(\zeta',\sigma')) = \mu_{a,\omega}(\zeta\,{}^\sigma\zeta',\sigma\sigma') &= \chi_a(\zeta\,{}^\sigma\zeta')\epsilon(\sigma\sigma')\omega^{u_\sigma+v_\sigma u_{\sigma'}}\theta_{v_\sigma v_{\sigma'}} \\ &= \chi_a(\zeta)\chi_a({}^\sigma\zeta')\epsilon(\sigma)\epsilon(\sigma')\omega^{u_\sigma+v_\sigma u_{\sigma'}}\theta_{v_\sigma v_{\sigma'}}. \end{aligned}$$

To prove these two quantities are equal, we need to show that $\chi_a({}^\sigma\zeta') = \chi_a(\zeta')^{v_\sigma}$:

$$\chi_a({}^\sigma\zeta') = \chi_{\sigma^{-1}a}(\zeta') = \chi_{v_\sigma a}(\zeta') = \chi_a(\zeta')^{v_\sigma}.$$

We now proceed to show that $\mu_{a,\omega}$ does not depends, up to isomorphism, on the choice of the representative $(a_1, \dots, a_n)$ of a such that each a_i is a multiple of f_a. If $(a'_1, \dots, a'_n)$ is another representative, there exists j such that $a'_i = a_i + jf_a$ for all i, and so

$$a'_{\sigma(i)} = a_{\sigma(i)} + jf_a = v_\sigma a_i + u_\sigma f_a + jf_a = v_\sigma a'_i + (u_\sigma + j(1 - v_\sigma))f_a.$$

Thus, $v'_\sigma = v_\sigma$ and $u'_\sigma = u_\sigma + j(1 - v_\sigma)$, hence

$$\mu'_{a,\omega}(\zeta,\sigma) = \chi_a(\zeta)\epsilon(\sigma)\omega^{u_\sigma+j(1-v_\sigma)}\theta_{v_\sigma} = \omega^j\mu_{a,\omega}(\zeta,\sigma)\,\omega^{-j}. \qquad \square$$

We now study the extension of scalars $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$. We use the isomorphism t from §3.1 between $\boldsymbol{\mu}_n(\mathbb{F}_q)$ and $\boldsymbol{\mu}_n(\overline{\mathbb{Q}}_\ell)$; there exists a unique embedding ι_a of $\mathbb{K}_a$ in $\overline{\mathbb{Q}}_\ell$ such that the following diagram is commutative:

$$\begin{tikzcd} E_a \arrow[r, hook] \arrow[d, equal] & \boldsymbol{\mu}_n(\mathbb{F}_q) \arrow[r, hook, "t"] & \boldsymbol{\mu}_n(\overline{\mathbb{Q}}_\ell) \arrow[d, hook] \\ E_a \arrow[r, hook] & \mathbb{K}_a \arrow[r, hook, "\iota_a"'] & \overline{\mathbb{Q}}_\ell \end{tikzcd}.$$

This embedding only depends on $\bar{a}$, not on a. Moreover, if we identify $a \in \hat{A}$ to a character $A \to \boldsymbol{\mu}_n(\mathbb{F}_q)$, the following diagram is commutative:

$$\begin{tikzcd} A \arrow[r, hook, "a"] \arrow[d, equal] & \boldsymbol{\mu}_n(\mathbb{F}_q) \arrow[r, hook, "t"] & \boldsymbol{\mu}_n(\overline{\mathbb{Q}}_\ell) \arrow[d, hook] \\ A \arrow[r, hook, "\chi_a"'] & \mathbb{K}_a \arrow[r, hook, "\iota_a"'] & \overline{\mathbb{Q}}_\ell \end{tikzcd}.$$

In the remainder of this §5.4, we identify $\mathbb{K}_a$ to the subfield $\iota_a(\mathbb{K}_a)$ of $\overline{\mathbb{Q}}_\ell$ thanks to ι_a.

With this identification, we have an isomorphism

$$\begin{aligned} \delta\colon\ \mathbb{K}_a \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell &\xrightarrow{\sim} \overline{\mathbb{Q}}_\ell^{(\mathbb{Z}/n_a\mathbb{Z})^\times} \\ k \otimes \lambda \quad &\mapsto (\theta_v(k)\lambda)_{v \in (\mathbb{Z}/n_a\mathbb{Z})^\times} \end{aligned}$$

Because

$$\begin{aligned} k \otimes \lambda &\xmapsto{\mu_{a,\omega}(\zeta,\sigma)\otimes \mathrm{Id}_{\overline{\mathbb{Q}}_\ell}} \chi_a(\zeta)\epsilon(\sigma)\omega^{u_\sigma}\theta_{v_\sigma}(k) \otimes \lambda \\ &\xmapsto{\quad\quad\delta\quad\quad} (\chi_a(\zeta)^v \epsilon(\sigma)\omega^{vu_\sigma}\theta_{vv_\sigma}(k)\lambda)_{v \in (\mathbb{Z}/n_a\mathbb{Z})^\times}, \end{aligned}$$

the endomorphism of $\overline{\mathbb{Q}}_\ell^{(\mathbb{Z}/n_a\mathbb{Z})^\times}$ deduced from $\mu_{a,\omega}(\zeta,\sigma) \otimes \mathrm{Id}_{\overline{\mathbb{Q}}_\ell}$ by the isomorphism δ is given by

$$(x_v)_{v \in (\mathbb{Z}/n_a\mathbb{Z})^\times} \mapsto (\chi_{va}(\zeta)\epsilon(\sigma)\omega^{vu_\sigma} x_{vv_\sigma})_{v \in (\mathbb{Z}/n_a\mathbb{Z})^\times}. \tag{5.1}$$

Proposition 5.10. *Let u_a be the homomorphism $\sigma \mapsto u_\sigma$ of S_a into $e_a\mathbb{Z}/n_a\mathbb{Z}$; it does not depend on the choice of the representative $(a_1, \ldots, a_n)$ of a and we have $u_{ka} = ku_a$ for all $k \in (\mathbb{Z}/n_a\mathbb{Z})^\times$ (see Remarks 5.8.c and 4.5.c). The $\overline{\mathbb{Q}}_\ell[A \rtimes S_{\bar{a}}]$-module $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ is isomorphic to*

$$\bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times / \operatorname{Im} k_a} \operatorname{Ind}_{A \rtimes S_a}^{A \rtimes S_{\bar{a}}}(ka \otimes \epsilon \otimes \omega^{u_{ka}}).$$

Proof. Formula (5.1) above shows that the isotypic components of the $\overline{\mathbb{Q}}_\ell[A]$-module $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ are of the form ka for $k \in (\mathbb{Z}/n_a\mathbb{Z})^\times$ (as in §3.1, we identify a to a character taking values in $\overline{\mathbb{Q}}_\ell$); each of these isotypic components is a direct sum of representations of dimension 1 isomorphic to ka.

Let's now determine the action of the group S_a. As $S_{ka} = S_a$ for all $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, the group S_a stablizes each one-dimensional piece isomorphic to ka of the $\overline{\mathbb{Q}}_\ell[A]$-module $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ and, by Formula (5.1), S_a acts on a piece isomorphic to ka by multiplication by $\epsilon(\sigma)\omega^{ku_\sigma} = \epsilon(\sigma)\omega^{u_{ka}}$.

This shows that the $\overline{\mathbb{Q}}_\ell[A \rtimes S_a]$-module $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ is isomorphic to

$$\bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} (ka \otimes \epsilon \otimes \omega^{u_{ka}}). \tag{5.2}$$

From Formula (5.1) and the fact that $S_{\bar a}/S_a = \operatorname{Im} k_a = \{v_\sigma \mid \sigma \in S_{\bar a}\}$, we have the following isomorphism of $\overline{\mathbb{Q}}_\ell[A \rtimes S_{\bar a}]$-modules:

$$\bigoplus_{k \in \operatorname{Im} k_a} (ka \otimes \epsilon \otimes \omega^{u_{ka}}) \simeq \operatorname{Ind}_{A \rtimes S_a}^{A \rtimes S_{\bar a}} (a \otimes \epsilon \otimes \omega^{u_a}).$$

From this, we get the announced result. ☐

We deduce the following three corollaries.

Corollary 5.11. *Up to isomorphism, $M_{a,\omega}$ only depends on the ${d_a}^{th}$ root of unity ω^{e_a}. More precisely,*

$$M_{a,\omega} \simeq M_{a',\omega'} \iff a' \in (\mathbb{Z}/n\mathbb{Z})^\times a \quad \textit{and} \quad \omega^{e_a} = \omega'^{e_a}.$$

Proof. As two representations isomorphic after extension of scalars are also isomorphic before (see [Curtis and Reiner, 1962, Theorem 29.7, page 200]), we only have to show the result for $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$. From Formula (5.2), we have

$$M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell|_A \simeq \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} ka,$$

which shows that, if $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \simeq M_{a',\omega'} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$, then $a' \in (\mathbb{Z}/n\mathbb{Z})^\times a$. Let us now assume that $a' \in (\mathbb{Z}/n\mathbb{Z})^\times a$ so that $e_a = e_{a'}$. Recall (see Remark 5.8.b as well as the proof of Proposition 4.4) that u_a is a surjection of S_a onto $e_a\mathbb{Z}/n_a\mathbb{Z}$ with $u_{ka} = ku_a$. By Formula (5.2), we have

$$M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell|_{S_a} \simeq \epsilon \otimes \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} \omega^{ku_a},$$

hence, if $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \simeq M_{a',\omega'} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$, we have $\{\omega^{ku_a} \mid k \in (\mathbb{Z}/n_a\mathbb{Z})^\times\} = \{\omega'^{ku_a} \mid k \in (\mathbb{Z}/n_a\mathbb{Z})^\times\}$ and so there exists $\kappa \in (\mathbb{Z}/n_a\mathbb{Z})^\times$ such that $\omega^{e_a} = \omega'^{\kappa e_a}$.

Conversely, we assume that $a' \in (\mathbb{Z}/n\mathbb{Z})^\times a$ and that there exists $\kappa \in (\mathbb{Z}/n_a\mathbb{Z})^\times$ such that $\omega^{e_a} = \omega'^{\kappa e_a}$ and prove that $M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \simeq M_{a',\omega'} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ if and only if $\kappa = 1$. We write $a' = k'a$ so that we have an isomorphism of $\overline{\mathbb{Q}}_\ell[A \rtimes S_a]$-modules

$$\begin{aligned} M_{a',\omega'} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell &\simeq \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} (kk'a \otimes \epsilon \otimes \omega'^{u_{kk'a}}) \\ &= \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} (\kappa ka \otimes \epsilon \otimes \omega'^{u_{\kappa ka}}) \\ &= \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} (\kappa ka \otimes \epsilon \otimes \omega^{u_{ka}}). \end{aligned}$$

This shows that $M_{a',\omega'} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \simeq M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ implies $\kappa = 1$. Conversely, if $\kappa = 1$, the isomorphism from Proposition 5.10 shows that

$$\begin{aligned} M_{a',\omega'} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell &\simeq \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times / \operatorname{Im} k_a} \operatorname{Ind}_{A \rtimes S_a}^{A \rtimes S_{\bar a}} (kk'a \otimes \epsilon \otimes \omega^{u_{kk'a}}) \\ &\simeq \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times / \operatorname{Im} k_a} \operatorname{Ind}_{A \rtimes S_a}^{A \rtimes S_{\bar a}} (ka \otimes \epsilon \otimes \omega^{u_{ka}}) \\ &\simeq M_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell. \end{aligned}$$

☐

Corollary 5.12. *For each ${d_a}^{th}$ root of unity $\eta \in \mathbb{K}_a$, we denote by $\omega(\eta) \in \mathbb{K}_a$ a ${n_a}^{th}$ root of unity satisfying $\omega(\eta)^{e_a} = \eta$. We have an isomorphism of $\mathbb{Q}_\ell[A \rtimes S_{\bar a}]$-modules*

$$\bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} M_{a,\omega(\eta)} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \simeq \bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times / \operatorname{Im} k_a} \operatorname{Ind}_{A \rtimes S_a}^{A \rtimes S_{\bar a}} (ka \otimes \epsilon \otimes \operatorname{reg}_{S_a/S'_a}).$$

Proof. According to the previous proposition, we only have to check that, for all $k \in (\mathbb{Z}/n_a\mathbb{Z})^\times$,

$$\bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} \omega(\eta)^{u_{ka}} = \mathrm{reg}_{S_a/S'_a}.$$

From Remark 5.8.*b*, we may write $u_a = e_a u'_a$ where $u'_a \colon S_a \to \mathbb{Z}/d_a\mathbb{Z}$ is a group homomorphism. We have $u'_a(\sigma) = 0 \iff u_a(\sigma) = 0 \iff \sigma \in S'_a$ as $j_a = -f_a u_a$ (Remark 5.8.*c*). Consequently, if $\sigma \in S_a$,

$$\begin{aligned}\sum_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} \omega(\eta)^{u_{ka}(\sigma)} = \sum_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} \omega(\eta)^{k u_a(\sigma)} &= \sum_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} \eta^{k u'_a(\sigma)} \\ &= \begin{cases} d_a & \text{if } \sigma \in S'_a, \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

which proves the announced result. □

Corollary 5.13. *We keep the notations of the previous corollary. We have an isomorphism of* $\mathbb{Q}_\ell[G]$*-modules*

$$H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}} \simeq \bigoplus_{a \in (\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n \backslash \hat{A}} m'_a \operatorname{Ind}^G_{A \rtimes S_{\bar{a}}} \Bigg(\bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} M_{a,\omega(\eta)} \Bigg) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Proof. As a consequence of the previous corollary and of the results of §4.8, we have

$$H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}} \simeq \bigoplus_{a \in (\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n \backslash \hat{A}} m'_a \operatorname{Ind}^G_{A \rtimes S_{\bar{a}}} \Bigg(\bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} M_{a,\omega(\eta)} \Bigg) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell.$$

We deduce the announced result over $\mathbb{Q}_\ell$ thanks to the same argument as in Corollary 5.11: two representations isomorphic after extension of scalars are also isomorphic before. □

5.5 Endomorphism rings of the representations

Denote by $W_{a,\omega}$ the $\mathbb{Q}[G]$-module $\operatorname{Ind}^G_{A \rtimes S_{\bar{a}}} M_{a,\omega}$; the aim of this §5.5 is to show that it is a simple module and identify its endomorphism ring.

Theorem 5.14. *The* $\mathbb{Q}[G]$*-module* $W_{a,\omega}$ *is simple. Moreover, if we identify the group* $\mathrm{Gal}(\mathbb{K}_a/\mathbb{Q})$ *with* $(\mathbb{Z}/n_a\mathbb{Z})^\times$*, the endomorphism ring of* $W_{a,\omega}$ *identifies with the unique subfield* D_a *of* $\mathbb{K}_a$ *such that* $\mathrm{Gal}(\mathbb{K}_a/D_a) = \operatorname{Im} k_a$*. That is to say,* D_a *is the subfield of* $\mathbb{K}_a$ *consisting of the elements fixed by all the* θ_{v_σ} *for* $\sigma \in S_{\bar{a}}$*. In particular,* D_a *is commutative.*

Proof. Since a $\mathbb{Q}[G]$-module is simple if and only if its endomorphism ring is a division ring, we only need to show the second assertion.

We have $W_{a,\omega} = \operatorname{Ind}^G_{A \rtimes S_{\bar{a}}} M_{a,\omega}$ where $M_{a,\omega}$ is just $\mathbb{K}_a$ with the structure of $\mathbb{Q}[A \rtimes S_{\bar{a}}]$-module given by the representation $\mu_{a,\omega}$. We may write $W_{a,\omega} = \bigoplus_{s \in \mathfrak{S}_n/S_{\bar{a}}} sM_{a,\omega}$. From the definition of $S_{\bar{a}}$, each $sM_{a,\omega}$ is stable by A and the $\mathbb{Q}[A]$-modules $sM_{a,\omega}$ are disjoint. Consequently, the endomorphism ring of $W_{a,\omega}$ stabilizes $M_{a,\omega}$ and $u \mapsto u|_{M_{a,\omega}}$ defines an isomorphism between the endomorphism ring of $W_{a,\omega}$ and the endomorphism ring of the $\mathbb{Q}[A \rtimes S_{\bar{a}}]$-module $M_{a,\omega}$.

We now need to show that the endomorphism ring of the $\mathbb{Q}[A \rtimes S_{\bar{a}}]$-module $M_{a,\omega}$ is the subfield of $\mathbb{K}_a$ fixed by all the θ_{v_σ} for $\sigma \in S_{\bar{a}}$. The endomorphism ring of the $\mathbb{Q}[A]$-module $M_{a,\omega}$ is canonically isomorphic to $\mathbb{K}_a$ via $x \mapsto (\lambda \mapsto x\lambda)$ since the $\mathbb{Q}[A]$-module $M_{a,\omega}$ is $\mathbb{K}_a$. We deduce that the endomorphism ring of the $\mathbb{Q}[A \rtimes S_{\bar{a}}]$-module $M_{a,\omega}$ is the subfield of $\mathbb{K}_a$ consisting of the elements x such that $\lambda \mapsto x\lambda$ commutes with each $\mu_{a,\omega}(\zeta, \sigma)$ i.e. with each θ_{v_σ}. Because $\lambda \mapsto x\lambda$ commutes with θ_{v_σ} if and only if $\theta_{v_\sigma}(x) = x$, the ring $D_a = \operatorname{End}_{\mathbb{Q}[G]}(W_{a,\omega}, W_{a,\omega})$ is the subfield of $\mathbb{K}_a$ fixed by each θ_{v_σ} for $\sigma \in S_{\bar{a}}$. □

Remarks 5.15. *a*) The field D_a is independent of the choice of ω.

b) The field D_a has dimension $\frac{\phi(n_a)}{\#\mathrm{Im}\, k_a}$ over $\mathbb{Q}$. When $(\mathbb{Z}/n_a\mathbb{Z})^\times$ is cyclic (e.g. when n is prime and $n_a = n$), this dimension characterizes D_a.

c) As $(\mathbb{Z}/e_a\mathbb{Z})^\times \subset \mathrm{Im}\, k_a$, we have $D_a \subset \mathbb{K}'_a$ where $\mathbb{K}'_a$ is the subfield of $\mathbb{K}_a$ generated by the ${e_a}^{\text{th}}$ roots of unity. In general, $D_a \neq \mathbb{K}'_a$ as we may see by taking $n = 5$ and $a = [0, 0, 1, 1, 3]$: we have $n_a = e_a = 5$ and so $\mathbb{K}_a = \mathbb{K}'_a = \mathbb{Q}(\boldsymbol{\mu}_5)$ whereas $D_a = \mathbb{Q}(\sqrt{5})$ (this is the same example as in the footnote to page 15).

Examples 5.16. *a*) When $a = [0, \ldots, 0]$, we have $D_a = \mathbb{K}_a = \mathbb{Q}$.

b) When $n = 5$ and $\bar{a}$ is the class of $[0, 0, 0, 1, 4]$ or $[0, 0, 1, 1, 3]$, we have $D_a = \mathbb{Q}(\sqrt{5})$.

c) When $n = 7$, we have the following possibilities concerning D_a.

class of $\bar{a}$	D_a
$[0,0,0,0,0,0,0]$, $[0,1,2,3,4,5,6]$	$\mathbb{Q}$
$[0,0,0,0,1,2,4]$, $[0,0,1,1,3,3,6]$	$\mathbb{Q}(\sqrt{-7})$
$[0,0,0,0,0,1,6]$, $[0,0,0,1,1,1,4]$ $[0,0,0,1,1,6,6]$, $[0,0,0,1,2,5,6]$ $[0,0,1,1,3,4,5]$, $[0,0,1,1,2,4,6]$	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$
$[0,0,0,0,1,1,5]$, $[0,0,0,1,1,2,3]$	$\mathbb{Q}(\boldsymbol{\mu}_7)$

Theorem 5.17. *We have*

$$W_{a,\omega} \simeq W_{a',\omega'} \iff a \in ((\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n)a' \text{ and } \omega^{e_a} = \omega'^{e_a}.$$

Proof. As two representations isomorphic after extension of scalars are also isomorphic before (see [Curtis and Reiner, 1962, Theorem 29.7, page 200]), we only need to show the result for $W_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$. Following Proposition 5.10, we have

$$W_{a,\omega} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell = \bigoplus_{s \in \mathfrak{S}_n / S_{\bar{a}}} sM_{a,\omega} \otimes \overline{\mathbb{Q}}_\ell \simeq \bigoplus_{s \in \mathfrak{S}_n / S_{\bar{a}}} s \left(\bigoplus_{k \in (\mathbb{Z}/n_a\mathbb{Z})^\times} (ka \otimes \epsilon \otimes \omega^{u_{ka}}) \right).$$

If a and a' are the same mod the action of $(\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n$, this formula shows that $W_{a,\omega} \otimes \overline{\mathbb{Q}}_\ell$ and $W_{a',\omega'} \otimes \overline{\mathbb{Q}}_\ell$ are not isomorphic.

If $a \in ((\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n)a'$, as the group $A \rtimes S_{\bar{a}}$ stabilizes each copy of $sM_{a,\omega}$ an thus stabilizes $M_{a,\omega}$, we deduce, thanks to Corollary 5.11, that if $\omega^{e_a} \neq \omega'^{e_a}$, then $W_{a,\omega} \otimes \overline{\mathbb{Q}}_\ell$ and $W_{a',\omega'} \otimes \overline{\mathbb{Q}}_\ell$ are not isomorphic.

Finally, if $a \in ((\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n)a'$ and $\omega^{e_a} = \omega'^{e_a}$, then the previous formula shows that $W_{a,\omega} \otimes \overline{\mathbb{Q}}_\ell \simeq W_{a',\omega'} \otimes \overline{\mathbb{Q}}_\ell$. □

6 Consequence for the factorization of the zeta function

The aim of this §6 is to show that $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$ is a direct sum of subspaces stable by the Frobenius and to deduce a factorization of the zeta function of X_ψ. The idea of using this method comes from [Hulek et al., 2006, §6.2].

The subspaces we consider are the isotypic components of the $\mathbb{Q}[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$; after describing them in §6.1, we study in §6.2 how the Frobenius acts on them and deduce that the characteristic polynomial of the restriction of the Frobenius is an integer power $Q_{a,\omega}^{\gamma_a/d_a}$ of a polynomial $Q_{a,\omega}$ which has integer coefficients independent of ℓ (see §6.3). Finally, in §6.4, we deduce that the part of the zeta function of X_ψ corresponding to $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$ is the product over $a \in \hat{A}$ and $\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)$ of the polynomials $Q^{\gamma_a/d_a}_{a,\omega(\eta)}$ (see Corollary 5.12 for the definition of $\omega(\eta)$) and we show that each $Q_{a,\omega(\eta)}$ factors over the field D_a considered in §5.5. We end by explicitly treating the cases $n = 3$, 4, 5, and 7 in §6.5.

6.1 Isotypic decomposition of the $\mathbb{Q}_\ell[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$

The aim of this §6.1 is to express, in terms of the representations $W_{a,\omega}$ considered above, the isotypic components of the $\mathbb{Q}[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$. We keep the notations of §5.5.

Proposition 6.1. *Let ω be a $n_a{}^{th}$ root of unity. The $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module $V_{a,\omega} = \operatorname{Hom}_{\mathbb{Q}[G]}(W_{a,\omega}, H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}})$ is free of rank m'_a.*

Proof. By Corollary 5.13, we have

$$H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}} \simeq \bigoplus_{a \in (\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n \backslash \hat{A}} \Bigg(\bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} W^{m'_a}_{a,\omega(\eta)} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \Bigg).$$

We deduce the following isomorphisms of $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-modules:

$$\begin{aligned}
V_{a,\omega} &= \operatorname{Hom}_{\mathbb{Q}[G]}(W_{a,\omega}, H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}) \\
&\simeq \bigoplus_{a' \in (\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n \backslash \hat{A}} \Bigg(\bigoplus_{\eta' \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} \operatorname{Hom}_{\mathbb{Q}[G]}(W_{a,\omega}, W^{m'_{a'}}_{a',\omega(\eta')} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \Bigg) \\
&\simeq \operatorname{Hom}_{\mathbb{Q}[G]}(W_{a,\omega}, W^{m'_a}_{a,\omega} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \\
&\simeq (\operatorname{End}_{\mathbb{Q}[G]}(W_{a,\omega}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^{m'_a} \\
&\simeq (D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^{m'_a}.
\end{aligned}$$

This shows that $V_{a,\omega}$ is a free $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank m'_a. ☐

Corollary 6.2. *The map $w \otimes v \mapsto v(w)$ of $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ into $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$ is $\mathbb{Q}_\ell[G]$-linear and injective; its image is the $W_{a,\omega}$-isotypic component $H_{\bar{a},\omega}$ of the $\mathbb{Q}[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$.*

Proof. We refer the reader to [Bourbaki, 1958, §3.4, Proposition 9, page 33] and [Bourbaki, 1958, §1.5, Theorem 1.b, page 15]. ☐

Remark 6.3. The link between the $\overline{H}_\alpha$ from §4.1 and the isotypic components $H_{\bar{a},\omega}$ from the previous corollary is given by

$$\bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} H_{\bar{a},\omega(\eta)} \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \simeq \bigoplus_{\alpha \in (\mathbb{Z}/n_a\mathbb{Z})^\times / \operatorname{Im} k_a} \operatorname{Ind}^G_{A \rtimes S_a} \overline{H}_\alpha.$$

6.2 Action of the Frobenius on each isotypic component

Lemma 6.4. *The Frobenius stablizes the $\mathbb{Q}_\ell[G]$-modules $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$.*

Proof. As all the elements of G are automorphisms of X_ψ defined over $\mathbb{F}_q$, the Frobenius endomorphism on $H^{n-2}_{\text{et}}(X_\psi, \mathbb{Q}_\ell)$ commutes with the action of G; it thus stabilizes each isotypic components of the $\mathbb{Q}[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$, namely, each of the $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ (Corollary 6.2). ☐

Proposition 6.5. *The Frobenius acts on $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ by $\operatorname{Id} \otimes v_{a,\omega}$ where $v_{a,\omega}$ is the endomorphism $v \mapsto \operatorname{Frob}^* \circ v$ of the $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module $V_{a,\omega}$.*

Proof. The action of the Frobenius on $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ is given by

$$\begin{aligned}\mathrm{Frob}^*(w \otimes v) &= \mathrm{Frob}^*(v(w)) = (\mathrm{Frob}^* \circ v)(w) = v_{a,\omega}(v)(w) = w \otimes v_{a,\omega}(v) \\ &= (\mathrm{Id} \otimes v_{a,\omega})(w \otimes v).\end{aligned}$$

The structure of $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of $V_{a,\omega} = \mathrm{Hom}_{\mathbb{Q}[G]}(W_{a,\omega}, H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}})$ is given by $(d \otimes \lambda)v = \lambda(v \circ d)$. We have

$$\mathrm{Frob}^* \circ (\lambda(v \circ d)) = \lambda(\mathrm{Frob}^* \circ v) \circ d,$$

and hence the map $v_{a,\omega}$ is an endomorphism of the $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module $V_{a,\omega}$. □

We deduce the following result, which describes the reciprocal polynomial of the characteristic polynomial of the Frobenius on each isotypic component.

Proposition 6.6. *Let ω be a ${n_a}^{th}$ root of unity, and set*

$$\begin{aligned}P_{a,\omega}(t) &= \det(1 - tv_{a,\omega} | V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \in D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell[t];\\ Q_{a,\omega}(t) &= N_{D_a \otimes \mathbb{Q}_\ell[t]/\mathbb{Q}_\ell[t]}(P_{a,\omega}(t)) \in \mathbb{Q}_\ell[t].\end{aligned}$$

We have $\deg P_{a,\omega} = m'_a$ and $\deg Q_{a,\omega} = \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} m'_a$. The reciprocal polynomial of the characteristic polynomial of the Frobenius over $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ is given by

$$\det(1 - t\,\mathrm{Frob}^* | W_{a,\omega} \otimes_{D_a} V_{a,\omega}) = Q_{a,\omega}(t)^{\gamma_a/d_a},$$

where γ_a is the number of permutations of $(a_1, \ldots, a_n)$ and d_a is the integer defined in §4.2.

Proof. As Frob^* acts on $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ by $\mathrm{Id} \otimes v_{a,\omega}$, we have [Bourbaki, 1970, §8.6, Example 3, page 101]

$$\begin{aligned}&\det(1 - t\,\mathrm{Frob}^* | W_{a,\omega} \otimes_{D_a} V_{a,\omega}/\mathbb{Q}_\ell)\\ &\qquad = \det(1 - tv_{a,\omega} | V_{a,\omega}/\mathbb{Q}_\ell)^{\dim_{D_a} W_{a,\omega}}\\ &\qquad = \det(1 - tv_{a,\omega} | V_{a,\omega}/\mathbb{Q}_\ell)^{(\dim_{\mathbb{Q}} W_{a,\omega})/[D_a:\mathbb{Q}]},\end{aligned}$$

with [Bourbaki, 1970, §9.4, Proposition 6, page 112]

$$\det(1 - tv_{a,\omega} | V_{a,\omega}/\mathbb{Q}_\ell) = N_{D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell[t]/\mathbb{Q}_\ell[t]}(\det(1 - tv_{a,\omega} | V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)),$$

which shows the announced formula given the following remarks:

a) the degree of the polynomial $P_{a,\omega}(t)$ is $m'_a = \dim_{D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell} V_{a,\omega}$;

b) the degree of the polynomial $Q_{a,\omega}(t)$ is $[D_a : \mathbb{Q}] \cdot \deg P_{a,\omega} = \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} m'_a$;

c) the dimension of $W_{a,\omega}$ over $\mathbb{Q}$ is $\phi(n_a)[\mathfrak{S}_n : S_a] = \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \frac{\gamma_a}{d_a} = \frac{\gamma_a}{d_a}[D_a : \mathbb{Q}]$, and thus $\frac{\dim_{\mathbb{Q}} W_{a,\omega}}{[D_a : \mathbb{Q}]} = \frac{\gamma_a}{d_a}$. □

6.3 Rationality and independence of ℓ of the characteristic polynomials

The aim of this §6.3 is to show that the polynomials $Q_{a,\omega}$ defined in Proposition 6.6 have rational coefficients an are independent of ℓ. We start with the following lemma, which we will use a couple of times in what follows.

Lemma 6.7. *Let E be a finite dimensional vector space over $\mathbb{Q}_\ell$ and u an endomorphism of E. The polynomial $\det(1 - tu)$ is an element of $\mathbb{Q}[t]$ independent of ℓ if and only if for all $r \geq 1$ the number $\mathrm{tr}(u^r)$ belongs to $\mathbb{Q}$ and is independent of ℓ.*

Proof. This is a straightforward consequence both of Viete's formulas (relating roots and coefficients of a polynomial) and of Newton's formulas. $\square$

The following lemma allows us to relate the independence of ℓ of $Q_{a,\omega}$ to that of $Q_{a,\omega}(t)^{\gamma_a/d_a}$.

Lemma 6.8. *Let $P \in 1 + t\mathbb{Q}[t]$ be a non-constant polynomial and $\gamma \in \mathbb{N}^*$. If, for each ℓ, there is a $Q_\ell \in 1 + t\mathbb{Q}_\ell[t]$ such that $Q_\ell^\gamma = P$, then Q_ℓ belongs to $1 + t\mathbb{Q}[t]$ and is independent of ℓ.*

Proof. Denote by $\sqrt[\gamma]{P}$ the unique element of $1 + t\mathbb{Q}[[t]]$ such that $(\sqrt[\gamma]{P})^\gamma = P$. We have $Q_\ell^\gamma = (\sqrt[\gamma]{P})^\gamma = P$ with $Q_\ell \in 1 + t\mathbb{Q}_\ell[[t]]$, which shows, as $\sqrt[\gamma]{P}$ is unique in $1 + t\mathbb{Q}_\ell[[t]]$, that $Q_\ell = \sqrt[\gamma]{P}$. Consequently, Q_ℓ belongs to $1 + t\mathbb{Q}[t]$ and is independent of ℓ. $\square$

We now deal with the independence of ℓ of $Q_{a,\omega}(t)^{\gamma_a/d_a}$ thanks to an argument of projector.

Proposition 6.9. *For each $a \in \hat{A}$, the polynomial $Q_{a,\omega}(t)^{\gamma_a/d_a}$ has rational coefficients and is independent of ℓ.*

Proof. Denote by $\xi_a \colon g \in G \mapsto \operatorname{tr}(g^*|W_{a,\omega}/\mathbb{Q})$ the character of the simple $\mathbb{Q}[G]$-module $W_{a,\omega}$. There is a projection π_a of $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$ onto $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ of the form

$$\pi_a = \frac{\lambda}{\#G} \sum_{g \in G} \xi_a(g^{-1}) g^*, \qquad \text{avec } \lambda \in \mathbb{Q},$$

where λ is computed by taking the trace of both members of the equality

$$\dim_{\mathbb{Q}} W_{a,\omega} = \frac{\lambda}{\#G} \sum_{g \in G} \xi_a(g^{-1}) \xi_a(g) = \lambda [D_a : \mathbb{Q}].$$

(Indeed, over $\overline{\mathbb{Q}}_\ell$, ξ_a is the direct sum of $[D_a : \mathbb{Q}]$ irreducible characters as we have seen in §5.) We thus have $\lambda = \dim_{D_a} W_{a,\omega}$.

Because the image of the projection π_a is $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$, we have

$$Q_{a,\omega}(t)^{\gamma_a/d_a} = \det(1 - t(\pi_a \circ \operatorname{Frob}^*)|H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}).$$

Using Lemma 6.7, we only have to show that the powers of $\pi_a \circ \operatorname{Frob}^*$ have a trace belonging to $\mathbb{Q}$ and independent of ℓ. This results from the fact that these powers can be written as linear combinations with coefficients in $\mathbb{Q}$ of quantities of the type f^* where f is an endomorphism of the variety X_ψ which extends to $\mathbb{P}^{n-1}$ and from the following lemma, which is an adaptation of [Katz and Messing, 1974, Theorem 2.2, page 76] to the case of traces over the primitive part of the cohomology of an irreducible hypersurface (since $n \geq 3$, X_ψ is irreducible). $\square$

Lemma 6.10. *Let X be a non-singular, irreducible hypersurface of $\mathbb{P}^{n-1}$. If $f \colon X \to X$ is an endomorphism of X which extends into an endomorphism of $\mathbb{P}^{n-1}$, then $\operatorname{tr}(f^*|H^{n-2}_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)^{\text{prim}})$ is an integer which is independent of ℓ.*

Proof. We have $H^{n-2}_{\text{et}}(\overline{X}, \mathbb{Q}_\ell) \simeq H^{n-2}_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)^{\text{prim}} \oplus H^{n-2}_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)^{\text{inprim}}$ with $\operatorname{tr}(f^*|H^{n-2}_{\text{et}}(\overline{X}, \mathbb{Q}_\ell))$ and $\operatorname{tr}(f^*|H^{n-2}_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)^{\text{inprim}}) = \operatorname{tr}(f^*|H^{n-2}_{\text{et}}(\mathbb{P}^{n-1}_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell))$ two integers independent of ℓ by [Katz and Messing, 1974, Theorem 2.2, page 76][3]. $\square$

Combining Lemma 6.8 and Proposition 6.9, we deduce the announced result.

Theorem 6.11. *The polynomials $Q_{a,\omega}(t)$ have rational coefficients and are independent of ℓ.*

In §6.4, we will see a stronger result, namely that the polynomials $P_{a,\omega}$ are independent of ℓ.

[3] On this subject, see also [Deligne and Lusztig, 1976, page 119] and [Illusie, 2006, §3.5, pages 112–113].

6.4 Factorization of the zeta function

From the preceding results, we can deduce a factorization over $\mathbb{Q}$ of the zeta function as well as the existence of a decomposition of some of the factors over finite extensions of $\mathbb{Q}$.

Theorem 6.12. *The zeta function of the hypersurface X_ψ of $\mathbb{P}^{n-1}_{\mathbb{F}_q}$ defined by $x_1^n + \cdots + x_n^n - n\psi x_1 \ldots x_n = 0$ (with $\psi \in \mathbb{F}_q^*$ satisfying $\psi^n \neq 1$) factors over $\mathbb{Q}$ as*

$$Z_{X_\psi/\mathbb{F}_q}(t) = \frac{\left(\prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times\times\mathfrak{S}_n\backslash\hat{A},\ \eta\in\boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} Q_{a,\omega(\eta)}(t)^{\gamma_a/d_a}\right)^{(-1)^{n-1}}}{(1-t)(1-qt)\ldots(1-q^{n-2}t)}.$$

(The notations are those of Corollary 5.12 and Proposition 6.6.)

Proof. The previous formula is just a reformulation of the results from §§6.1, 6.2 and 6.3. □

Remarks 6.13. *a*) Let us recall that the factor corresponding to $[0, 1, 2, \ldots, n-1]$ does not intervene (see Remark 3.5 page 7).

b) The polynomials $Q_{a,\omega}$ depend on ω^{e_a}. See Example 6.20 page 27.

c) When n is a prime number (necessarily odd, as $n \geq 3$), we have $d_a = 1$ if $a \neq [0, 1, 2, \ldots, n-1]$, and thus $\omega(\eta) = 1$; hence, in that case, the numbers $\omega(\eta)$ don't intervene.

d) As we mentioned in the introduction, a similar result of factorization was proved by R. Kloosterman in a slightly different context, see [Kloosterman, 2007, Corollary 6.10, page 448]. The factorization he obtains is a bit coarser as it involves the polynomials $R_a(t) = \prod_\eta Q_{a,\omega(\eta)}(t)$; we refer the reader to Example 6.20 for an illustration of this phenomenon.

We now look how the polynomials $Q_{a,\omega}$ behave over the field D_a.

Proposition 6.14. *The polynomials $Q_{a,\omega}$ factor over D_a as a product of $[D_a : \mathbb{Q}]$ polynomials of degree m'_a.*

Proof. As $Q_{a,\omega}(t) = N_{D_a\otimes\mathbb{Q}_\ell[t]/\mathbb{Q}_\ell[t]}(P_{a,\omega}(t))$, the polynomial $Q_{a,\omega}$ is the product of the conjugates of $P_{a,\omega}$. □

The following theorem shows that this factorization is independent of ℓ.

Theorem 6.15. *The polynomials $P_{a,\omega}$ have coefficients in D_a and are independent of ℓ.*

Proof. Let us recall that $P_{a,\omega}(t) = \det(1 - tv_{a,\omega}|V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$. Using the same argument as in Lemma 6.7, we only need to show the independence of ℓ of $\mathrm{tr}(v^r_{a,\omega}|V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ for every $r \in \mathbb{N}$.

As $(x, y) \mapsto \mathrm{Tr}_{D_a\otimes_{\mathbb{Q}}\mathbb{Q}_\ell/\mathbb{Q}_\ell}(xy)$ is a non-degenerate bilinear form, the independence of ℓ of $\mathrm{tr}(v^r_{a,\omega}| V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ is equivalent to that of the element $\mathrm{tr}(dv^r_{a,\omega}|V_{a,\omega}/\mathbb{Q}_\ell) \in \mathbb{Q}_\ell$ for all $d \in D_a$; indeed:

$$\begin{aligned}\mathrm{Tr}_{D_a\otimes_{\mathbb{Q}}\mathbb{Q}_\ell/\mathbb{Q}_\ell}&\left(d\,\mathrm{tr}(v^r_{a,\omega}|V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)\right)\\ &= \mathrm{Tr}_{D_a\otimes_{\mathbb{Q}}\mathbb{Q}_\ell/\mathbb{Q}_\ell}\left(\mathrm{tr}(dv^r_{a,\omega}|V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)\right)\\ &= \mathrm{tr}(dv^r_{a,\omega}|V_{a,\omega}/\mathbb{Q}_\ell).\end{aligned}$$

Because $dv^r_{a,\omega}$ is the map $v \mapsto (\mathrm{Frob}^*)^r \circ v \circ d$, thanks to Remark 6.18, we only need to show the following proposition. □

Proposition 6.16. *Let X be a smooth projective variety over $\mathbb{F}_q$. Let G be a finite subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(X/\mathbb{F}_q)$, W a simple $\mathbb{Q}[G]$-module, D (the opposite of) its endomorphism ring, and i an integer ≥ 0. Denote by V the $D\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module $\mathrm{Hom}_{\mathbb{Q}[G]}(W, H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell))$ and, given $d \in D$ and $r \geq 1$, denote by α the endomorphism $v \mapsto (\mathrm{Frob}^*)^r \circ v \circ d$ of the $\mathbb{Q}_\ell$-vector space V. The trace of α is an element of $\mathbb{Q}$ which is independent of ℓ.*

Proof. Denote by E the $\mathbb{Q}_\ell$-vector space $\mathrm{Hom}_{\mathbb{Q}}(W, H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell))$, the action of G on E being $g \cdot v = g^* \circ v \circ g_W^{-1}$ where g_W is the endomorphism of the $\mathbb{Q}$-vector space W induced by g. Let π be the $\mathbb{Q}_\ell$-linear map from E to itself defined by

$$\pi(v) = \frac{1}{\#G} \sum_{g \in G} g^* \circ v \circ g_W^{-1}.$$

It is a projection with image $E^G = V$. The map $\beta \colon v \mapsto (\mathrm{Frob}^*)^r \circ v \circ d$ is an endomorphism of the $\mathbb{Q}_\ell$-vector space E which stabilizes V; the endomorphism of V induced by β is α and, because π is a projection of E onto V, we have

$$\mathrm{tr}(\alpha) = \mathrm{tr}(\pi \circ \beta),$$

where the endomorphism $\pi \circ \beta$ can be written as

$$v \mapsto \sum_{i \in I} (\mathrm{Frob}^*)^r \circ g_i^* \circ v \circ f_i,$$

with I a finite set, g_i some elements of G and f_i some endomorphisms of the $\mathbb{Q}$-vector space W, each of them independent of ℓ. We thus only need to show the following lemma. $\square$

Lemma 6.17. *We keep the notations of the previous proposition. If $g \in G$, $f \in \mathrm{End}_{\mathbb{Q}}(W)$ and $r \in \mathbb{N}^*$, then the trace of*

$$v \mapsto (\mathrm{Frob}^*)^r \circ g^* \circ v \circ f$$

considered as an endomorphism of V is an element of $\mathbb{Q}$ independent of ℓ.

Proof. Let $(e_1, \dots, e_k)$ be a basis of W over $\mathbb{Q}$; the map

$$v \mapsto (v(e_1), \dots, v(e_k))$$

is an isomorphism of the $\mathbb{Q}_\ell$-vector space V onto the $\mathbb{Q}_\ell$-vector space $H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell)^k$. It sends the endomorphism of V given by

$$v \mapsto (\mathrm{Frob}^*)^r \circ g^* \circ v \circ f$$

to the endomorphism of $H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell)^k$ given by

$$(h_1, \dots, h_k) \mapsto \left(\sum_{i=1}^k a_{i,j} ((\mathrm{Frob}^*)^r \circ g^*)(h_i) \right)_{1 \le j \le k},$$

where $(a_{i,j})_{1 \le i,j \le k}$ is the matrix of f in the basis $(e_i)_{1 \le i \le k}$. Its trace is thus equal to

$$\left(\sum_{i=1}^k a_{i,i} \right) \mathrm{tr}((\mathrm{Frob}^*)^r \circ g^* | H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell)).$$

By [Katz and Messing, 1974, Theorem 2.2, page 76], it is independent of ℓ. $\square$

Remark 6.18. In the previous lemma and proposition, it is possible, when X is a hypersurface, to replace $H^{n-2}_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell)$ by $H^{n-2}_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell)^{\mathrm{prim}}$ using Lemma 6.10 instead of [Katz and Messing, 1974, Theorem 2.2, page 76] (indeed, Frob^* and each g^*, with $g \in G$, extend to $\mathbb{P}^{n-1}$).

6.5 Examples

In this §6.5, we detail the computations for the cases $n = 3$, $n = 4$, $n = 5$, and $n = 7$. In all these examples, we use the fact that, when n is prime and $a \neq [0, 1, 2, \ldots, n-1]$, we have $\omega = 1$ and $d_a = 1$, hence $m'_a = m_a$ and $\gamma_a/d_a = \gamma_a$. Let us recall that the degree of $Q_{a,\omega}$ is $(\deg P_{a,\omega})[D_a : \mathbb{Q}] = m'_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a}$. In the tables, the lines appear by decreasing values of m_a.

Example 6.19 ($n = 3$)**.** This is the simplest non-trivial case. The elements of $\hat{A}$ are, up to permutation, $[0, 0, 0]$ and $[0, 1, 2]$. The multiplicity of the latter is zero so only $[0, 0, 0]$ gives rise to a factor in the zeta function. This factor has degree $m'_a = 2$ and appears with a power $\gamma_a/d_a = \gamma_a = 1$, so

$$Z_{/\mathbb{F}_q}(t) = \frac{Q_{[0,0,0],1}(t)}{(1-t)(1-qt)}, \qquad \text{with} \quad \deg Q_{[0,0,0],1}(t) = 2.$$

In fact, in this case, $\overline{X}_\psi$ is an elliptic curve, so the previous result doesn't give any new information.

Example 6.20 ($n = 4$)**.** Here is a list of the elements of $\hat{A}$ mod the simultaneous actions of $\mathfrak{S}_n$ and $(\mathbb{Z}/n\mathbb{Z})^\times$

class of $\bar{a}$	$\deg Q_{a,\omega}$	γ_a/d_a	D_a	ω
$[0, 0, 0, 0]$	3	1	$\mathbb{Q}$	1
$[0, 0, 2, 2]$	1	3	$\mathbb{Q}$	± 1
$[0, 0, 1, 3]$	1	12	$\mathbb{Q}$	1

Consequently, we have the following factorization of the zeta function:

$$Z_{/\mathbb{F}_q}(t) = \frac{1}{(1-t)(1-qt)(1-q^2t)} \times \frac{1}{Q_{[0,0,0,0],1}(t) Q_{[0,0,2,2],1}(t)^3 Q_{[0,0,2,2],-1}(t)^3 Q_{[0,0,1,3],1}(t)^{12}}.$$

This result is in accordance with the numerical observations of [Kadir, 2004, §6.1.1, pages 112–116]; let us note that, according to her tables for $q = p = 13, 17, 29, 37, 41$ (we remind the reader that only the cases $q \equiv 1 \mod 4$ fall in the framework of our study) and $\psi = 2, 3, 2, 2, 2$ respectively, we have $\{Q_{[0,0,2,2],1}(t), Q_{[0,0,2,2],-1}(t)\} = \{1 - pt, 1 + pt\}$, hence the two polynomials $Q_{[0,0,2,2],1}$ and $Q_{[0,0,2,2],-1}$ are not generally equal.

This example also illustrate the fact that our method gives a slightly finer factorization than that of Kloosterman [2007]: instead of finding a factor $R^3_{[0,0,2,2]}$ with $R_{[0,0,2,2]}$ of degree 2, we find a factor $Q_{[0,0,2,2],1}(t)^3 Q_{[0,0,2,2],-1}(t)^3$ with $Q_{[0,0,2,2],1}$ and $Q_{[0,0,2,2],-1}$ of degree 1; thus, Kloosterman's polynomial $R_{[0,0,2,2]}$ factors over $\mathbb{Q}$ as a product of two polynomials of degree 1.

Example 6.21 (Cas $n = 5$)**.** Here are all the elements of $\hat{A}$ (mod the simultaneous actions of $\mathfrak{S}_n$ and $(\mathbb{Z}/n\mathbb{Z})^\times$) which intervene in the zeta function:

class of $\bar{a}$	$\deg Q_{a,1}$	γ_a/d_a	D_a
$[0, 0, 0, 0, 0]$	4	1	$\mathbb{Q}$
$[0, 0, 0, 1, 4]$	4	20	$\mathbb{Q}(\sqrt{5})$
$[0, 0, 1, 1, 3]$	4	30	$\mathbb{Q}(\sqrt{5})$

We can thus write:

$$Z_{/\mathbb{F}_q}(t) = \frac{Q_{[0,0,0,0,0],1}(t) Q_{[0,0,0,1,4],1}(t)^{20} Q_{[0,0,1,1,3],1}(t)^{30}}{(1-t)(1-qt)(1-q^2t)(1-q^3t)}.$$

Moreover, the polynomials $Q_{[0,0,0,1,4],1}$ and $Q_{[0,0,1,1,2],1}$ factor over $D_a = \mathbb{Q}(\sqrt{5})$ into a product of two polynomials of degree 2 (namely, the corresponding $P_{a,1}$ and its conjugate over $\mathbb{Q}(\sqrt{5})$).

We thus recover (and explain) the numerical observation that Candelas, de la Ossa and Rodriguez-Villegas made in [Candelas et al., 2003, Table 12.1, page 133][4].

Example 6.22 (Cas $n = 7$)**.** The elements of $\hat{A}$ mod the simultaneous actions of $\mathfrak{S}_n$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ are those given in Example 5.16.c page 21. We complete the list with the useful informations concerning the factorization of the zeta function.

class of $\bar{a}$	$\deg Q_{a,1}$	γ_a/d_a	D_a
$[0,0,0,0,0,0,0]$	6	1	$\mathbb{Q}$
$[0,0,0,0,0,1,6]$	12	42	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$
$[0,0,0,0,1,1,5]$	24	105	$\mathbb{Q}(\boldsymbol{\mu}_7)$
$[0,0,0,1,1,1,4]$	12	140	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$
$[0,0,0,1,1,6,6]$	12	210	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$
$[0,0,0,0,1,2,4]$	6	210	$\mathbb{Q}(\sqrt{-7})$
$[0,0,0,1,1,2,3]$	18	420	$\mathbb{Q}(\boldsymbol{\mu}_7)$
$[0,0,1,1,3,3,6]$	6	630	$\mathbb{Q}(\sqrt{-7})$
$[0,0,0,1,2,5,6]$	6	840	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$
$[0,0,1,1,3,4,5]$	6	1260	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$
$[0,0,1,1,2,4,6]$	6	1260	$\mathbb{Q}(\boldsymbol{\mu}_7)^+$

As in the preceding cases, from this table, we can easily describe the factorization of the zeta function in the case $n = 7$.

Acknowledgments

I would like to thank my thesis advisor, Joseph Oesterlé, for sharing his ideas with me and for the numerous improvements he suggested to the text of the present article. I would also like to thank Luc Illusie for a helpful reference concerning Theorem 2.1 as well as Julien Grivaux for his elegant proof of Lemma 2.5.

A List of notations

General notations

$\#E$	number of elements of E
$\mathbb{F}_q$	finite field with q elements
$\mathbb{Q}_\ell$	field of ℓ-adic numbers
$\overline{\mathbb{K}}$	algebraic closure of the field $\mathbb{K}$
$\boldsymbol{\mu}_n(\Bbbk)$	set of n^{th} roots of unity belonging to the field $\Bbbk$
ϕ	Euler totient function
$\mathfrak{S}_n$	permutation group of $\{1,\ldots,n\}$
ϵ	signature (of a permutation)
$\operatorname{Ind}_H^G \mu$	representation of G induced by the representation μ of H
$[\![1;n]\!]$	set of integers k satisfying $1 \leq k \leq n$

Notations from the introduction

ψ	parameter belonging to $\mathbb{F}_q^*$	p. 1
δ_i	$\delta_i = 0$ if i is even and $\delta_i = 1$ if i is odd	p. 1
A	group $\{(\zeta_1,\ldots,\zeta_n) \in \boldsymbol{\mu}_n(\mathbb{F}_q)^n \mid \zeta_1\ldots\zeta_n = 1\}$ quotiented by $\{(\zeta,\ldots,\zeta)\}$; is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{n-2}$	p. 1

[4] As mentioned in the introduction, they only make this observation in the case $\psi = 0$, but their numerical data supports it when $\psi \neq 0$ and $q \equiv 1 \mod 5$.

$\hat{A}$	group $\{(a_1, \ldots, a_n) \in (\mathbb{Z}/n\mathbb{Z})^n \mid a_1 + \cdots + a_n = 0\}$ quotiented by the diagonal $\{(a, \ldots, a)\}$; can be identified with the group of characters of A	p. 1
$[\zeta_1, \ldots, \zeta_n]$	element of A	p. 1
$[a_1, \ldots, a_n]$	element of $\hat{A}$	p. 1
G	group $A \rtimes \mathfrak{S}_n$	p. 2

Notations from §2

X^f	subscheme of fixed point of an automorphism f of X	p. 3
$\chi(X)$	Euler–Poincaré characteristic of a scheme X	p. 3
$H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)^{\mathrm{inprim}}$	non-primitive part of the cohomology of a hypersurface of dimension $n-2$; is zero when the dimension is odd	p. 3
$H^{n-2}_{\mathrm{et}}(X, \mathbb{Q}_\ell)^{\mathrm{prim}}$	primitive part of the cohomology of a hypersurface of dimension $n-2$	p. 3

Notations from §3.

$k(\zeta)$	number of $i \in \{1, \ldots, n\}$ such that $\zeta_i = \zeta$	p. 5
m_a	multiplicity of the character a in the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(\overline{X}_\psi, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$	p. 5

Notations from §4.

$\overline{H}_a$	a-isotypic component of the $\overline{\mathbb{Q}}_\ell[A]$-module $H^{n-2}_{\mathrm{et}}(X, \overline{\mathbb{Q}}_\ell)^{\mathrm{prim}}$; its dimension is m_a	p. 7
G_a	stabilizer of a in G	p. 7
$\langle a \rangle$	orbit of $a \in \hat{A}$ under $\mathfrak{S}_n$	p. 7
R	representative set $\subset \hat{A}$ of the elements of $\mathfrak{S}_n \backslash \hat{A}$	p. 7
S_a	stabilizer of a in $\mathfrak{S}_n$	p. 7
n'_a	generator $\in [\![1; n]\!]$ of the set of elements $j \in \mathbb{Z}/n\mathbb{Z}$ such that $(a_1 + j, \ldots, a_n + j)$ is a permutation of $(a_1, \ldots, a_n)$	p. 8
d_a	integer equal to n/n'_a	p. 8
$I(b)$	set of $i \in [\![1; n]\!]$ such that $a_i = b$	p. 8
σ	element of S_a belonging to the preimage of a generator of the cyclic group S_a/S'_a	p. 8
S'_a	stabilizer in $\mathfrak{S}_n$ of a representative $(a_1, \ldots, a_n)$ of a in $(\mathbb{Z}/n\mathbb{Z})^n$	p. 8
γ_a	number of permutations of $(a_1, \ldots, a_n)$; equal to $[\mathfrak{S}_n : S'_a]$	p. 8
$\overline{\Sigma}_a$	group generated by σ; we have $S_a = S'_a \rtimes \overline{\Sigma}_a$	p. 8
j_a	group homomorphism $S_a \to n'_a\mathbb{Z}/n\mathbb{Z}$ defined by ${}^s(a_1, \ldots, a_n) = (a_1 + j_a(s), \ldots, a_n + j_a(s))$; satisfies $j_{ka} = kj_a$	p. 8
$\hat{A}^\sigma$	set of elements of $\hat{A}$ fixed by $\sigma \in \mathfrak{S}_n$	p. 9
O_j	orbits of a product of n' disjoint cycles of length d	p. 10
$k(\zeta)$	number of $j \in \{1, \ldots, n'\}$ such that $\prod_{i \in O_j} \zeta_i = \zeta$; this notation generalizes that from p. 5	p. 10
m'_a	$m'_a = m_a/d_a$	p. 14
reg	regular representation of S_a/S'_a	p. 14

Notations from §5

$\mathbb{K}_C$	cyclotomic field attached to a cyclic group C	p. 15
χ_C	canonical character of a cyclic group C; takes its values in $\mathbb{K}_C$	p. 15
$\bar{a}$	class mod $(\mathbb{Z}/n\mathbb{Z})^\times$ of a	p. 15
E_a	image of the homomorphism $[\zeta_1, \ldots, \zeta_n] \mapsto \zeta_1^{a_1} \ldots \zeta_n^{a_n}$	p. 15
N_a	kernel of the homomorphism $[\zeta_1, \ldots, \zeta_n] \mapsto \zeta_1^{a_1} \ldots \zeta_n^{a_n}$	p. 15
n_a	order of a in $\hat{A}$; equal to the order of the group generated by $a_i - a_{i'}$; also equal to the number of elements of the image of the character a	p. 15

$\mathbb{K}_a$	cyclotomic field attached to the cyclic group A/N_a; its dimension over $\mathbb{Q}$ is $\phi(n_a)$; only depends on $\bar{a}$	p. 15
χ_a	canonical character of the cyclic group A/N_a considered as a character of A; takes values in $\mathbb{K}_a$ and satisfies $\chi_{ka} = \chi_a^k$	p. 15
f_a	generator of the group generated by $a_i - a_{i'}$; satisfies $n'_a = e_a f_a$, $n = e_a f_a d_a$ and $n = n_a f_a$	p. 15
$S_{\bar{a}}$	fixator of $\bar{a}$ in $\mathfrak{S}_n$	p. 15
k_a	group homomorphism $S_{\bar{a}} \to (\mathbb{Z}/n_a\mathbb{Z})^\times$ defined by ${}^\sigma a = k_a(\sigma)a$; only depends on $\bar{a}$	p. 15
e_a	integer such that $n'_a = e_a f_a$; satisfies $n_a = e_a d_a$ and $n = e_a f_a d_a$	p. 16
(u_σ, v_σ)	if $\sigma \in S_{\bar{a}}$, unique pair $(u_\sigma, v_\sigma) \in \mathbb{Z}/n_a\mathbb{Z} \times (\mathbb{Z}/n_a\mathbb{Z})^\times$ such that $a_{\sigma(i)} = v_\sigma a_i + u_\sigma f_a$	p. 16
ϕ	group homomorphism $S_{\bar{a}} \to \mathbb{Z}/n_a\mathbb{Z} \rtimes (\mathbb{Z}/n_a\mathbb{Z})^\times$, $\sigma \mapsto (u_\sigma, v_\sigma)$; we have $v_\sigma = k_a(\sigma)$ and $f_a u_\sigma = j_a(\sigma)$	p. 16
θ_v	automorphism of the field $\mathbb{K}_a$ sending the ${n_a}^{\text{th}}$ roots of unity to their v^{th} power	p. 17
ω	${n_a}^{\text{th}}$ root of unity	p. 17
$\mu_{a,\omega}$	representation $(\zeta, \sigma) \mapsto \chi_a(\zeta)\epsilon(\sigma)\omega^{u_\sigma}\theta_{v_\sigma}$ of $A \rtimes S_{\bar{a}}$ in $\mathbb{K}_a$	p. 17
$M_{a,\omega}$	$\mathbb{Q}[A \rtimes S_{\bar{a}}]$-module $\mathbb{K}_a$ given by $\mu_{a,\omega}$; up to isomorphism, only depends on ω^{e_a}, not on ω	p. 17
$W_{a,\omega}$	$\mathbb{Q}[G]$-module simple $\mathrm{Ind}_{A \rtimes S_{\bar{a}}}^G M_{a,\omega}$	p. 20
D_a	(opposite of the) endomorphism ring of $W_{a,\omega}$; we have $D_a \subset \mathbb{K}_a$ (hence D_a is commutative) and $\dim_{\mathbb{Q}} D_a = \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a}$	p. 20

Notations from §6

$V_{a,\omega}$	$\mathrm{Hom}_{\mathbb{Q}[G]}(W_{a,\omega}, H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}})$; is a free $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank m'_a; $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$ identifies with the $W_{a,\omega}$-isotypic component $H_{\bar{a},\omega}$ of the $\mathbb{Q}[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$	p. 22
$H_{\bar{a},\omega}$	$W_{a,\omega}$-isotypic component of the $\mathbb{Q}[G]$-module $H^{n-2}_{\text{et}}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\text{prim}}$; is isomorphic to $W_{a,\omega} \otimes_{D_a} V_{a,\omega}$	p. 22
$v_{a,\omega}$	endomorphism of the $D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module $V_{a,\omega}$ such that $\mathrm{Frob}^* \vert W_{a,\omega} \otimes_{D_a} V_{a,\omega} = \mathrm{Id} \otimes v_{a,\omega}$	p. 22
$P_{a,\omega}$	polynomial $\det(1 - tv_{a,\omega} \vert V_{a,\omega}/D_a \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ having degree m'_a; has coefficients in D_a and is independent of ℓ	p. 23
$Q_{a,\omega}$	polynomial $N_{D_a \otimes \mathbb{Q}_\ell[t]/\mathbb{Q}_\ell[t]}(P_{a,\omega}(t))$ having degree $m'_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a}$ and coefficients in $\mathbb{Q}$; is independent of ℓ	p. 23

B Formulas

Here is a list of the most important formulas established throughout this article.

$n = n'_a d_a = e_a f_a d_a = n_a f_a$, $n'_a = e_a f_a$, and $n_a = e_a d_a$.

$[\mathfrak{S}_n : S'_a] = \gamma_a$ (number of permutations of $(a_1, \ldots, a_n)$)

$$[\mathfrak{S}_n : S_a] = \frac{\gamma_a}{d_a}$$

$$[\mathfrak{S}_n : S_{\bar{a}}] = \frac{\gamma_a}{\#(\mathrm{Im}\, k_a) d_a}$$

$$[S_a : S'_a] = d_a$$

$$[S_{\bar a} : S_a] = \#\mathrm{Im}\, k_a \qquad (\text{in fact, } S_{\bar a}/S_a = \mathrm{Im}\, k_a)$$

$$[S_{\bar a} : S'_a] = d_a \#\mathrm{Im}\, k_a$$

$$\dim \overline{H}_a = m_a$$

$$\dim \mu_{a,\omega} = \dim M_{a,\omega} = \dim \mathbb{K}_a = \phi(n_a)$$

$$\dim M_{a,\omega}^{m'_a} = m'_a \phi(n_a)$$

$$\dim W_{a,\omega}^{m'_a} = \dim \mathrm{Ind}_{A \rtimes S_{\bar a}}^G M_{a,\omega}^{m'_a} = m'_a \phi(n_a)[\mathfrak{S}_n : S_{\bar a}] = m'_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \frac{\gamma_a}{d_a}$$

$$\dim \bigoplus_{\eta \in \boldsymbol{\mu}_{d_a}(\mathbb{K}_a)} \mathrm{Ind}_{A \rtimes S_{\bar a}}^G M_{a,\omega(\eta)}^{m'_a} = m_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \frac{\gamma_a}{d_a}.$$

$$\dim_{\mathbb{Q}} D_a = \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a}$$

$$\dim_{\mathbb{Q}}(W_{a,\omega}) = \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \frac{\gamma_a}{d_a} = [\mathfrak{S}_n : S_a][D_a : \mathbb{Q}].$$

$$\dim_{D_a}(V_{a,\omega}) = m'_a.$$

$$\dim_{\mathbb{Q}}(H_{\bar a,\omega}) = m'_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \frac{\gamma_a}{d_a} = m'_a [\mathfrak{S}_n : S_a][D_a : \mathbb{Q}]$$

$$\dim_{\mathbb{Q}_\ell}(H_{\mathrm{et}}^{n-2}(\overline{X}_\psi, \mathbb{Q}_\ell)^{\mathrm{prim}}) = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n \backslash \hat{A}} m'_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \gamma_a = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times \times \mathfrak{S}_n \backslash \hat{A}} m_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a} \frac{\gamma_a}{d_a}.$$

$$\deg P_{a,\omega} = m'_a$$

$$\deg Q_{a,\omega} = (\deg P_{a,\omega})[D_a : \mathbb{Q}] = m'_a \frac{\phi(n_a)}{\#\mathrm{Im}\, k_a}$$

References

N. Bourbaki. *Algèbre, chapitre VIII.* Hermann, 1958.

N. Bourbaki. *Algèbre, chapitre III.* Hermann, new edition, 1970.

L. Brünjes. *Forms of Fermat Equations and Their Zeta Functions.* World Scientific, 2004.

P. Candelas, X. de la Ossa, and F. Rodriguez-Villegas. Calabi-Yau Manifolds over Finite Fields, II. In N. Yui and J. D. Lewis, editors, *Calabi-Yau Varieties and Mirror Symmetry*, volume 38 of *Fields Institute Comm. Series*, pages 121–157, Toronto, July 23-29, 2001, 2003. Fields Institute, AMS.

G. Chênevert. Representations on the Cohomology of Smooth Projective Hypersurfaces with Symmetries. *Preprint*, 2009. Available at `http://arxiv.org/abs/0908.1748`.

C. W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras.* Interscience, 1962.

P. Deligne and G. Lusztig. Representations of Reductive Groups Over Finite Fields. *Annals of Math.*, 103:103–161, 1976.

E. Freitag and R. Kiehl. *Etale Cohomology and the Weil Conjecture*. Springer, 1988.

K. Hulek, R. Kloosterman, and M. Schütt. Modularity of Calabi-Yau varieties. In Catanese, Esnault, Huckleberry, Hulek, and Peternell, editors, *Global aspects of complex geometry*, pages 271–309, 2006.

L. Illusie. Miscellany on traces in ℓ-adic cohomology: a survey. *Japanese Journal of Mathematics, 3rd series*, 1:107–136, 2006.

S. N. Kadir. *The Arithmetic of Calabi–Yau Manifolds and Mirror Symmetry*. PhD thesis, Oxford University, 2004. Available at `http://arxiv.org/abs/hep-th/0409202`.

N. M. Katz. Another Look at the Dwork Family. In Y. Tschinkel, editor, *Algebra, Arithmetic and Geometry – Manin Festschrift*, pages 85–122, 2009. Currently available at `http://www.math.princeton.edu/~nmk/dworkfamilyfinal.pdf`.

N. M. Katz and W. Messing. Some Consequences of the Riemann Hypothesis for Varieties over Finite Fields. *Invent. Math.*, 23:73–77, 1974.

R. Kloosterman. The zeta-function of monomial deformations of Fermat hypersurfaces. *Algebra & Number Theory*, 1:421–450, 2007.

SGA5. *Cohomologie ℓ-adique et fonction L (SGA 5)*, volume 589 of *Lecture notes in mathematics*. Springer, 1965–1966. Séminaire de Géométrie Algébrique du Bois-Marie, dirigé par A. Grothendieck avec la collaboration de I. Bucur, C. Houzel, L. Illusie, J.-P. Jouanolou et J.-P. Serre.